

U. S. DEPARTMENT OF ENERGY

**INSTRUMENTATION, CONTROLS
AND HUMAN-MACHINE INTERFACE
(IC&HMI) TECHNOLOGY WORKSHOP
Gaithersburg, Maryland
May 2002**

**Don W. Miller
Edward L. Quinn
Steven A. Arndt
Leonard J. Bond
Donald B. Jarrell
John M. O'Hara
Richard T. Wood**

U. S. DEPARTMENT OF ENERGY

**INSTRUMENTATION, CONTROLS
AND HUMAN-MACHINE INTERFACE
(IC&HMI) TECHNOLOGY WORKSHOP
Gaithersburg, Maryland
May 2002**

Published: September 2002

**Don W. Miller
Edward L. Quinn
Steven A. Arndt
Leonard J. Bond
Donald B. Jarrell
John M. O'Hara
Richard T. Wood**

TABLE OF CONTENTS

ACRONYMS	v
1.0 INTRODUCCION	1
2.0 BACKGROUND	3
2.1 DOE Budget Requests	3
2.2 NERAC's Roadmap	3
2.3 The Nuclear Power 2010 Initiative	3
2.4 The Nuclear Power 2010 Initiative and Ongoing Activities	4
2.5 Institutional Challenges	5
3.0 INSTRUMENTATION, CONTROLS AND HUMAN-MACHINE INTERFACE (IC & HMI) TECHNOLOGY WORKSHOP SESSION REPORTS	7
3.1 Sensors and Measurement Systems.....	7
3.1.1 Session Participants and Goals	7
3.1.2 Overview of the State of Sensor and Measurement System Technology	7
3.1.3 Issues and Needs for Sensors and Measurement Systems Technology	9
3.1.4 Recommendations	11
3.1.5 References for Sensors and Measurement Systems	11
3.2 Diagnostics and Prognostics.....	12
3.2.1 Session Participants and Goals.....	12
3.2.2 Overview of the State of Diagnostics and Prognostics Technology	12
3.2.3 Issues and Needs for Diagnostics and Prognostics Technology	16
3.2.4 Recommendations	18
3.2.5 References for Diagnostics and Prognostics	20
3.3 Computational Methods	22
3.3.1 Session Participants and Goals	22
3.3.2 Overview of the State of Computational Methods Technology	22
3.3.3 Issues and Needs for Computational Methods Technology	24
3.3.4 Recommendations	26
3.3.5 References for Computational Methods	27
3.4 Computing and Communications Architectures	27
3.4.1 Session Participants and Goals	27
3.4.2 Overview of the State of Computing and Communications Architectures Technology	27
3.4.3 Issues and Needs for Computing and Communications Architectures Technology ..	31
3.4.4 Recommendations	33
3.5 Human-System Interactions	34
3.5.1 Session Participants and Goals	34
3.5.2 Overview of the State of Human-System InteractionsTechnology	34
3.5.3 Issues and Needs for Human-System Interactions Technology	35
3.5.4 Recommendations	40
3.6 Regulatory Framework.....	41
3.6.1 Session Participants and Goals	41
3.6.2 Overview of the State of Regulatory Framework.....	41
3.6.3 Issues and Needs for Regulatory Framework.....	43
3.6.4 Recommendations	46
4.0 MEETING RESEARCH NEEDS – A PROPOSED PATH FORWARD	47
4.1 High priority Projects, Facilities, and Tests Beds	47
4.1.1 Goal	47
4.1.2 Demonstration Program for NP 2010	47
4.1.3 Longer-term Research Areas Supporting Generation IV	48

ACRONYMS

ABWR	Advanced Boiling Water Reactor
ALMR	advanced liquid-metal reactor
ALWR	advanced light-water reactor
ANS	American Nuclear Society
ASME	American Society of Mechanical Engineers
ATR	advanced test reactor
COL	combined construction-operating license
COTS	commercial-off-the-shelf
CSCW	computer-supported cooperative work
D/P	diagnostics and prognostics
DC	design certification
DOE	U.S. Department of Energy
EMI/RFI	electromagnetic interference/radio-frequency interference
EPRI	Electric Power Research Institute
ESP	early site permit
GQM	goal/question/metric
HEART	hardened electronic and radiation technology
HSI	human-system interface
HTGR	high-temperature gas reactors
I&C	instrumentation and controls
IC&HMI	instrumentation, control, and human-machine interface
INEEL	Idaho National Engineering and Environmental Laboratory
ITAAC	inspection, testing, and analysis criteria
MSET	Multivariate State Estimation Technique
NEER	Nuclear Engineering Education Research
NERAC	Nuclear Energy Research Advisory Committee
NERI	DOE Nuclear Energy Research Initiative
NOB	normal operating band
NRC	Nuclear Regulatory Commission
NRR	Nuclear Reactor Regulation
ORNL	Oak Ridge National Laboratory
PLCs	programmable logic controllers
PRA	probabilistic risk assessment
PSP	personal software process
PWR	Pressurized Water Reactor
QIP	Quality Improvement Paradigm
RF	radio frequency
RFP	request for proposals
SWIFT	software implemented fault tolerance
TSP	team software process
V&V	verification and validation

1.0 INTRODUCCION

The Office of Nuclear Energy, Science, and Technology of the U.S. Department of Energy (DOE) sponsored a workshop to solicit input from nuclear power experts to its planning for research in this critical technology area in support of its Nuclear Power 2010 and Generation IV programs

The goal of workshop was establish the need to include instrumentation, control, and human-machine interface (IC&HMI) early in the design of Nuclear Power 2010 and Generation IV nuclear power plants. The Nuclear Energy Research Advisory Committee (NERAC) 1999 workshop report was used as a starting point, providing background for the current workshop discussions and serving as a reference point for this report that documents the workshop results and recommendations.

To accomplish this goal the following objectives of were identified:

- Develop a vision for IC&HMI over the next decade
- Identify technological issues related to IC&HMI for multi-modular plants employing Generation IV reactors
- Develop an integrated research plan to address critical technological issues in a systematic manner

The workshop had six breakout or working groups, which were chaired by members of the organizing committee:

1. Sensors and Measurement Systems—Don Miller
2. Diagnostics and Prognostics—Leonard Bond and Don Jarrell
3. Computational Methods—Richard Wood
4. Computing and Communications Architectures—Ted Quinn
5. Human-System Interaction—John O’Hara
6. Regulatory Framework—Steven Arndt

Prior to the conference, workshop participants were provided with documents to provide background information as a means of preparation.

2.0 BACKGROUND

The Nuclear Power 2010 Initiative boosts prospects for new plant orders in the United States. This workshop is a cooperative effort among various members of the instrumentation and controls (I&C) industrial sector to propose next generation nuclear plant design. The workshop members took into consideration DOE budget requests, NERAC's nuclear power plant roadmap, utility scoping studies, and a full-scale demonstration of the licensing process. This background information is briefly described in this section.

2.1 DOE BUDGET REQUESTS

The *Department of Energy FY 2003 Congressional Budget Request*, which was submitted in February, includes \$38.5 million for the Nuclear Power 2010 Initiative. The request relies heavily on the recommendations of NERAC, an independent advisory committee from industry, national laboratories, and universities.

The *DOE FY 2003 Congressional Budget Request* states:

The Department believes it is critical to deploy new baseload nuclear generating capacity within the next decade to support the National Energy Policy objectives of energy supply diversity and energy security. A major obstacle to the deployment of new nuclear power plants is the uncertainties associated with the federal regulatory processes and the financial and schedule risks resulting from these uncertainties. The Nuclear Power 2020 program is a joint government-industry, cost-shared activity to develop advanced reactor technologies and demonstrate new regulatory processes leading to initiation of private sector construction of new nuclear power plants in the United States in 2005.

2.2 NERAC'S ROADMAP

In October 2001, NERAC published its recommendations in the report, *Roadmap to Deploy New Nuclear Power Plants in the United States*. Although NERAC recommended \$62.5 million for FY 2003 activities relating to the roadmap, the nuclear industry considers \$38.5 million a step in the right direction. The DOE budget request for the 2010 Initiative reflects the near-term deployment section of the roadmap report. That section identified regulatory and institutional gaps that are barriers to plant orders in the near term. The report calls for demonstration of the regulatory licensing processes of 10 CFR Part 52 for early site permit, design certification (DC), and combined construction-operating license (COL). The report also calls for completion of the detailed design and engineering for at least one advanced light water reactor (ALWR) and at least one advanced gas-cooled reactor.

2.3 THE NUCLEAR POWER 2010 INITIATIVE

The Nuclear Power 2010 Initiative consists of two phases. Phase 1 is aimed at eliminating licensing uncertainties and obtaining design certification for two advanced nuclear power plant designs. Phase 2 is aimed at completing the detailed design and engineering work for two advanced-design nuclear power plants by 2005.

Last year, DOE issued a request for proposals (RFP) for cooperative projects to scope out sites for a possible early site permit (ESP) application. With ESP, an application is made to the Nuclear Regulatory Commission (NRC) for approval of a site for a possible future nuclear power plant. The site may be set aside so that it is ready if and when a decision is made to actually build a plant. When a new plant is needed, it can be ready sooner if the site is already licensed.

On February 14, 2002, Secretary Abraham announced that DOE has selected Exelon and Dominion Resources for the scoping projects. These utilities will conduct scoping studies of both private and federal sites for ESP. They will examine the NRC licensing process, as it would be applied for sites they own and also for federal government sites at Savannah River, the Idaho National Engineering and Environmental Laboratory, and the Portsmouth, Ohio site.

A third utility, Entergy, did not receive funding but is still expected to move forward with ESP and may receive funds when they become available for the next step, which is a full-scale demonstration of the licensing process for a selected site.

DOE announced its RFP for cost-shared, full-scale demonstrations on February 27, 2002. Three awards were made on June 20, 2002, to support ESP applications for Dominion, Entergy, and Exelon.

Early site permitting will be the biggest DOE-sponsored activity over the next year and a half. After that, the 2010 Initiative also envisions a cost-shared project to test the currently untested process to apply to the NRC for a COL for a new nuclear power plant. The aim is a real application as early as 2004/2005.

2.4 THE NUCLEAR POWER 2010 INITIATIVE AND ONGOING ACTIVITIES

The term Nuclear Power 2010 Initiative refers to DOE-funded projects that would begin in FY 2003, if Congress approves the funding. However, these projects are a continuation and expansion of ongoing DOE efforts.

DOE's plan includes the following elements, starting from FY 2001 (dates shown are fiscal years, which begin October 1 of the previous year):

- 2001 DOE began evaluating technical and institutional issues to be addressed for near-term deployment of new nuclear power plants.
- 2001 DOE began working with the NRC to develop a regulatory and licensing framework for gas-cooled reactors. This work continues in FY 2002.
- 2001 DOE began activities to commercialize the advanced gas-cooled reactor that was being developed for surplus weapons disposition, including fuel development and testing, plant cost evaluation, and evaluation of waste disposal issues. This work continues in FY 2002.
- 2002 NERAC roadmap study was completed.
- 2002 DOE awarded funds to Dominion and Exelon for cost-shared projects to scope out potential private and government sites for new nuclear power plants.
- 2002 DOE will begin cost-shared projects to for a full-scale demonstration of the NRC ESP process.
- 2002 DOE will begin cost-shared development and certification projects for enhanced advanced light water reactors and advanced gas-cooled reactors.
- 2002 DOE will seek joint-venture teams to participate in the Nuclear Power 2010 program. According to the FY 2003 budget document: "The purpose of these joint venture teams is to develop innovative business arrangements, such as consortia among designers,

constructors, reactor equipments suppliers, and plant owner/operators with strong and common incentives to successfully build and operate new plants in the United States. These activities will be cost-shared with industry contributing at least 50 percent of the costs. For the engineering and design activities, the Department will recover its investments through royalty payments on future reactor sales.”

- 2002 DOE will enter into a cooperative agreement with U.S. industry and international partners for a gas-cooled reactor fuel irradiation and qualification program, which will be finalized in 2002. Design and fabrication of irradiation test fixtures will be completed.
- 2002 DOE and the NRC, together with the vendors, will complete an initial evaluation of gas-cooled reactor technologies and technical and licensing issues.
- 2003 Cost-shared projects to demonstrate the NRC early site permit process will continue.
- 2003 Cost-shared design certification activities for one advanced light water reactor and one gas-cooled reactor will continue and will include all engineering and design needed to gain approval for the designs from the NRC and for commercial deployment.
- 2003 DOE will initiate cost-shared demonstration projects for at least two combined COL applications.
- 2003 Gas-cooled reactor fuel qualification projects will continue, and DOE will collaborate with NRC and private industry to begin irradiating gas-cooled reactor fuel at the Advanced Test Reactor (ATR) at the Idaho National Engineering and Environmental Laboratory (INEEL).

2.5 INSTITUTIONAL CHALLENGES

Gaining congressional support is not the only challenge to fulfilling the vision of the 2010 Initiative. At the R&D Summit, February 24–25, 2002, representatives of industry and government discussed a number of institutional challenges that need to be addressed collaboratively in support of new nuclear power plant development.

William D. Magwood, IV, Director of the DOE Office of Nuclear Energy, Science, and Technology, commented that the industry needs more long-term thinking. He said that DOE will help with “a lot of issues to be settled—regulatory issues such as NRC certification.” But he also said, “adding 10 to 20 plants is not much really. We need to see much more happen. We need to start thinking about the long-term issues, issues twenty years from now. The industry needs to have people thinking about these long-term issues.”

Mr. Magwood also advised the industry that, ultimately, DOE would like to see the industry coalesce around a limited number of technologies.

Major effort is needed to reinvigorate the national laboratory infrastructure, and Mr. Magwood asked for industry collaboration in this effort: “We need to think about nuclear energy at the labs in the long-term context. We need to spend more time working together. We do need each other—DOE and the industry. If we don’t bring back this infrastructure, the long-term future won’t be here when we need it.”

Mr. Magwood also said that nuclear power has the support of this Administration and the Secretary of Energy and that there is support for collaboration leading to deployment of more

nuclear power plants. He said, “We’re going to work closely with the industry to make sure we’re in sync.”

NEI President and CEO, Joe Colvin, agreed with Mr. Magwood that a long-term industry view is important. He said that institutional barriers exist because the companies that operate the nation’s nuclear power plants are electricity generators, and their job is to look at the economic issues. “Their long-term future is in the next quarter’s earnings,” he said. Mr. Colvin noted that fuel companies and, to some degree, architectural firms have a vested interest in the long-term future of nuclear power.

Richard Myers, NEI Senior Director of Business Operations, commented at the Summit that all these ongoing policy initiatives fundamentally are aimed at mitigating commercial risk. Success, he said, will be measured in making nuclear power a commercially sustainable business.

From the business perspective, Mr. Myers said, “Our timing as an industry is about right.” He also noted that, as the industry goes about testing the licensing process and planning for the future, “we need to remember our core values. We have a unique value. We have competitive electricity, with forward price stability, and with a clean air value. Only nuclear energy provides all three values.”

Mr. Myers also cautioned that the Enron scandal should not be associated uniquely with the energy field. “This was a business-related catastrophe rather than an energy-related catastrophe,” he said.

3.0 INSTRUMENTATION, CONTROLS AND HUMAN-MACHINE INTERFACE (IC&HMI) TECHNOLOGY WORKSHOP SESSION REPORTS

3.1 SENSORS AND MEASUREMENT SYSTEMS

3.1.1 Session Participants and Goals

3.1.1.1 Participants

Alan Beard, General Electric
Jeff Chivers, Rosemont
David Chichester Gamma-Metrics
Mike Dougherty, Rosemont
Herb Estrada, Caldon
Robert Fielder, Luna Innovations
Hash Hashemian, AMS
Ernie Hauser, Caldon
David Holcomb, Oak Ridge National Laboratory
George Mattingly, National Institute of Science and Technology
Don W. Miller, Ohio State University,
Frank Ruddy, Westinghouse Electric
Jeff Tuetken Gamma-Metrics

3.1.1.2 Goals

The primary goal of the measurement systems working group is to identify critical issues related to measurement systems and methods, both current and advanced, that measure the four fundamental physical variables—temperature, pressure, flow and nuclear power or flux—that are necessary to safely operate and control a nuclear power plant. In addition, other physical variables that are unique to Generation IV and are necessary for their safe operation and control are identified.

One important criterion is the capability to maintain measurement accuracy for extended operational times using minimum maintenance. This requirement implies maximum stability, reliability, and maintainability, which may be attained with smart sensors that can identify faults and can diagnose the system's tolerance to degradation and failure. These smart sensors may monitor either internal and external stressors.

This working group also considered measurement systems that require minimum use of copper wires for data pathway, using optical-based and wireless sensors instead of copper wires.

3.1.2 Overview of the State of Sensor and Measurement System Technology

Measurement Systems, which comprise the sensor and signal conditioning electronics in current operating nuclear power plants, have not changed appreciably since their original design in the 1950s. These systems depend on a variety of traditional process and radiation sensors for measuring safety parameters and controlling variables such as temperature (RTDs, thermocouples), pressure (diaphragm, piezoelectric), flow (differential pressure), and neutron flux (fission chambers, ion chambers).

Most power plants continue to use large coaxial cables for transmission of data (or data pathways) from the measurement instruments. A nuclear plant uses literally miles of cables and hundreds of specialized penetrations for cables going through containment or pressure-vessel walls.

The I&C systems in the ALWR designs (i.e., Generation III reactors) employ more advanced technology than current plants; however, these ALWRs do not incorporate new technology on a broad scale. Two exceptional applications of technology are the broad use of software-based digital systems and the use of fiber optics for signal isolation and data transmission in nonradioactive areas

As the industry considers I&C systems in Generation IV reactors, the opportunity exists to take a much less “timid” design philosophy than was taken in the design of I&C systems in the ALWRs.

The first consideration is data transmission— or more broadly data pathways—which is a form of communication. These new communication pathways do not transfer information by electrons flowing in copper wires. Virtually all new communication systems use an electromagnetic method (light, microwaves, HF, VHF radio signals) instead of copper wires. Generation IV nuclear power plants should minimize the use of copper wires for data transmission. Data should be transmitted primarily by fiber optics and various wireless methods, some of which can penetrate thick barriers. In addition to electromagnetic interference/radio-frequency interference (EMI/RFI) immunity, the widespread use of fiber optics and wireless methods for data transmission would simplify both I&C system design and overall plant design through minimal use of large cables for data transmission.

The second consideration is sensors. Optical and wireless methods should be used for data transmission, and optical-based and wireless methods should be used for sensors. The industry should also take advantage of microprocessors, which provide opportunities to embed “intelligence” in the sensor, thus increasing accuracy, reliability, stability, and tolerance to external stressors (i.e., sensitivity to radiation, humidity, smoke, and high temperature) (Hashemian 1998; Miller 1999).

Although the industry should consider optical and wireless-based sensors when available, we should also consider other methods. Several examples are itemized below.

- In the past several years, the use of acoustic methods, either transmission timing or correlation methods, have been developed to the point that they are being introduced as a backfit in operating plants (Regan 2000).
- Ruddy describes the use of silicon carbide semiconductor detectors as ex-core neutron monitors for pressurized water reactors (Ruddy et al. 2000).
- A new method for local measurement of reactor power by direct measurement of the nuclear energy deposition rather than neutron flux is being developed at Ohio State University (Radcliff 2000).
- Holcomb at Oak Ridge National Laboratory is proposing to develop a combined optical-based neutron flux/temperature sensor for in-core measurements in high-temperature gas reactors (HTGR) (Holcomb 2001).
- NUREG/CR-5501 (Hashemian 1998) addressed other advanced technologies that should be considered in the design of a monitoring system for a nuclear power plant.

3.1.3 Issues and Needs for Sensors and Measurement Systems Technology

The measurement systems working group identified the following issues and needs. With each need or issue is a brief discussion to describe the issue. A section on recommendations presents an approach to solve or close the issue. A majority of the issues are currently being addressed and require no additional research. The group recommends that the unresolved issues become elements of the integrated research plan

3.1.3.1 Radiation Environment

When developing new sensors, measurement systems, and data pathways one must include not only how the system operates but also an understanding of the environment in which the sensor and the primary system operate. An important and obvious environmental stressor in a nuclear power plant is radiation. Two critical issues identified by the working group were the reliability of radiation-hardened components and electronics and the standards for installation and operation of new electronics in radiation environments.

Measurement systems should be designed to minimize placing electronics in high radiation fields; however, situations exist where the optimum design requires the signal-processing electronics be located in radiation fields. Therefore, availability of qualified radiation-hardened electronics is needed as is an understanding of radiation effects and ways to compensate for them. However, prior to initiating a research program, ongoing programs such as the IEEE Radiation Effects and DOD/DOE Hardened Electronic and Radiation Technology (HEART) conferences should be considered a source of information on these topics.

3.1.3.2 Basic Materials Research

In order to design sensors and operate them reliability over extended periods of time, materials properties at high temperatures in the presence of high radiation fields must be better understood. For example, highly reliable electrical contacts, which would seem to be a well defined component, can be a potential “show stopper” if the change in materials properties when significant temperature changes occur is not understood.

3.1.3.3 Wide Bandwidth Data Pathways

Technology is available or being developed (e.g., Windows, RF wireless, acoustic, ultrasonic, fiber optic) that will provide improved bandwidth data pathways that reach through the reactor vessel and the containment.

3.1.3.4 Innovative Standards

Innovative standards are needed for in-situ verification of calibration, communication protocols and maintainability, expansion of commercial dedication, and data pathways. In developing standards for these technology areas, consideration should given to the application of commercial safety standards. Historically, standards have been developed on a voluntary basis with support by the individual’s respective employer and sponsored by a professional society. Unfortunately, with the extremely cost-competitive situation in the nuclear industry, volunteers are not readily available, and employer support is becoming increasingly difficult to come by. As a consequence, DOE and the industry need to recognize that development of standards will require substantial subsidy. The ongoing effort to develop probabilistic risk assessment (PRA) standards being sponsored by the American Society of Mechanical Engineers (ASME) and the American Nuclear Society (ANS) provides a good paradigm that DOE and the industry should consider.

3.1.3.5 High-temperature Sensors

The two high-temperature gas reactors require reliable in-core and ex-core high-temperature sensors. Important aspects in attaining long-term liability will depend on improved knowledge of materials at high temperatures and good standards for design and installation of sensors

3.1.3.6 Improved Sensor Functionality

Sensor functionality in the future should include (where appropriate) fault identification and diagnostics, compensation for external and internal stressors, prognostics, and in-situ testability (e.g., calibration, response time). Sensors and measurement systems should be designed where needed with embedded capability for remote communications and with user interfaces.

Increasing opportunities exist for using embedded microprocessors and innovative physics in the design of sensors and measurement systems. These microprocessors will enable simultaneous measurement of more than one physical variable. Therefore, development of multi-measuring sensors should become a design objective.

3.1.3.7 Flexible I&C Platforms

In the past two years, the NRC has certified three I&C platforms, and the NRC has approved revised Electric Power Research Institute (EPRI) guideline on digital upgrades. EPRI is planning to initiate a program on risk-informed digital upgrades, which will incorporate its guidance about digital upgrades. The issue of flexible I&C platforms should be resolved by considering the experience gained by plants planning to use certified platforms and the recommendations made by the EPRI risk-informed digital upgrades program. Therefore, no further action is recommended on this issue.

3.1.3.8 Identification of Critical Process Variables

Following consideration of the design concept-specific needs of selected advanced reactors (e.g., IRIS, PBMR), this working group identified the following critical process variables.

- Detection: He, Po, Xe, etc.
- Temperature, flow, fission products, particulates
- In-core and ex-core neutron flux
- Improved pressure measurements
- Bulk average temperature
- Severe accident instruments
- Coolability
- Recriticality monitoring
- Debris cooling

3.1.3.9 Wide-range, In-Vessel Flux Monitor

More than one in-core neutron flux and power monitor will be funded by the DOE Nuclear Energy Research Initiative (NERI) program. Therefore, additional research by DOE is not required.

3.1.3.10 Accuracy

The issue of accuracy is of highest priority and should be an important objective in a majority of the above critical technology issues.

3.1.3.11 Sensors and Measurement Systems for Nonoperational Needs

The working group identified needs for the following nonoperational sensors and measurement systems:

- Security (e.g. biometrics)
- Inspection, Testing, and Analysis Criteria (ITAAC)
- Fuel fabrication

3.1.4 Recommendations

- Build and make available test beds for research and development and sensor qualification
- Complete basic research required for sensor development and installation
 - Materials related to increased reliability at high temperatures and radiation hardening
 - Signal processing
 - Sensor communication pathways
 - Radiation-hardened electronics

3.1.5 References for Sensors and Measurement Systems

Hashemian, H. 1998. "*Advanced Instrumentation and Maintenance Technologies for Nuclear Power Plants*", NUREG/CR-5501, August.

Holcomb, D.A. 2001. Private Communication, January.

Miller, D.W. et al. 1999. "Fiber Optic Sensors in Nuclear Power Plant Radiation Environments," EPRI TR-107326, Vol. 1, February.

Radcliff, T., D.W. Miller and A.C Kauffman. 2000. "Constant-Temperature Calorimetry for In-core Power Measurement," *Nuclear Technology*, September.

Regan, J. and H. Estrada. 2000. "The Elements of Uncertainty In Feed Water Flow Measurements with Three Types of Instruments," ANS Topical Meeting, NPIC& HMIT 2000, Washington DC, November.

Ruddy, F.H, et al. 2000. "Nuclear Power Monitoring Using Silicon Carbide Semiconductor Radiation Detectors," ANS Topical Meeting, NPIC& HMIT 2000, Washington DC, November.

3.2 DIAGNOSTICS AND PROGNOSTICS

3.2.1 Session Participants and Goals

3.2.1.1 Participants

John Beatty, Westinghouse
John Bernard, Massachusetts Institute of Technology
Leonard Bond, Pacific Northwest National Laboratory
Robert Edwards, Penn State University
Wesley Hines, University of Tennessee, Knoxville
Don Jarrell, Pacific Northwest National Laboratory
Joel Kramer, Nuclear Regulatory Commission
Jose March-Leuba, Oak Ridge National Laboratory
Belle Upadhyaya, University of Tennessee, Knoxville

3.2.1.2 Goals

The goal of the diagnostics and prognostics (D/P) group was to examine the topics involved in the determination and forecasting of machinery health, and to identify needed capabilities for future D/P research and development. This contributes toward the overall IC&HMI goal of providing a topical needs statement and a roadmap for achieving an IC&HMI vision for future reactor designs.

3.2.2 Overview of the State of Diagnostics and Prognostics Technology

To meet Generation IV goals of safe and economic operation for a next generation nuclear power plant, advanced and automated diagnostics and prognostics will be required. These technologies will enable safer and more reliable operation and extended intervals between outages to be achieved. Integration of multiple sensor data outputs through data fusion will provide signals for control and fault diagnostics of actuators and predictions of system element remaining life. The use of prognostics will provide for a proactive approach to operations and maintenance issues that reduce unplanned outages, optimize staff utilization, and that will result in smart self-diagnostic systems that operate with high reliability.

The fault diagnosis process in any form of abstraction contains at least the following information elements (Jarrell 1991):

- Recognition of problem existence
- Localization of the fault
- Fault specification—complete fault description
- Root cause determination—correlates the behavioral deviation from the design basis of the failed component/system.

Various diagnostic approaches and solution methodologies that perform these tasks were examined in this session.

Prognostics is an emerging discipline in which the estimation of physical degradation rate and remaining useful life is inferred based on sensor data information transforms. This information can then be used to effectively manage the facility assets and schedule maintenance on an as-needed rather than on an elapsed-time basis.

Recent developments in computer technology are now enabling a newly developed generation of D/P technologies to be implemented. These systems provide residual life prognostics based on sensor measurements and real-time data analysis and give an assessment of current condition state as well as time to failure. These “on-line, intelligent, self-diagnostic technologies,” merge

smart sensors, distributed data processing, advanced communication architectures, and data transmission technologies (e.g., wireless technologies) to give robust systems that provide current sensor and machine condition assessment as well as accurate machinery failure prognostics. Several projects that address aspects of these technologies are currently supported under the DOE NERI Program [<http://neri.ne.doe.gov/>].

Current technologies include a wide array of approaches that are in various states of maturity. These methodologies include the following:

- Trending and statistical techniques
- Data fusion
- Expert systems
- Data-driven solutions
- Stressor-based D/P—the integral damage model
- Hybrid systems

3.2.2.1 Trending and Statistical Techniques

The most common (and most mature) procedure used to deal with understanding degradation and failure prediction involves the trending of an index or parameter that relates to the performance of the equipment. Figure 3.2.1 shows a performance index that starts to decline from its normal operating band (NOB), reaches an alert level, and is subsequently analyzed to try to understand a reasonable projection for residual life. Failure is defined as the point at which the equipment is no longer capable of supporting the function for which it was designed. Associated with this method is a large cone of time to failure uncertainty that is created by extending the maximum and minimum slope of the trend until it reaches the predetermined failure level.

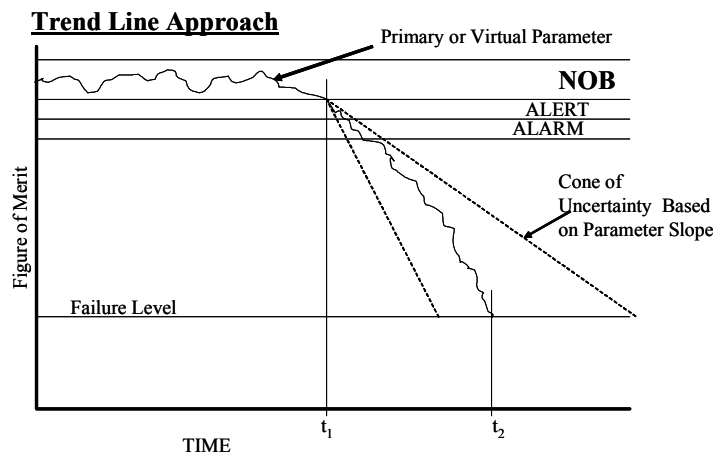


Fig. 3.2.1. Time line approach to failure prediction.

3.2.2.2 Data Fusion

Data fusion is the seamless integration of data from disparate sources to identify an anomalous process behavior. The data must be integrated across data collection “platforms” and geographic boundaries and blended thematically so that the differences in resolution and coverage, treatment of a theme, character, and artifacts of data collection methods are eliminated. Thus, this approach

attempts to integrate multiple input parameters into a single dynamic that provides a superior indicator of process anomalies. Diagnostics to determine the nature of the anomaly can then apply through various pattern-matching techniques or statistical approaches.

3.2.2.3 Expert Systems

The primary purpose of expert systems is to capture the human capability of diagnosis and control for particularly difficult or specialized tasks (Waterman 1986). If-then-else rules are the building blocks of expert systems. These rules permit conditional decision making in which the outcome decision is based on the logical condition of input variables. The strategy is to make a rule-based system flexible enough to cope with the many degrees of freedom that arise in large complex systems but manageable to design and test. By subdividing the system into smaller subsystems, the development workload can be shared and performed in parallel; nevertheless, the human effort to design large-scale expert systems is large. Domain expertise and computer logic familiarity are prime prerequisites for such systems to be effective. This technology is probably the second most mature in terms of breadth of application.

3.2.2.4 Data-Driven Solutions

This category of solutions attempts to identify process anomalies by establishing a signature norm for a process and using that norm to construct a predictive envelope against which operating data is compared. Deviations from the prediction envelope are flagged as indicators of current or developing problems. Often called inverse problems, they are modeling techniques that learn system behavior through data acquired from that system. This category of solutions is probably the most complex and least developed of the D/P approaches, is data intensive (hence data driven or data-based model), and in its current state of development, produces inconsistent results. Data-driven systems are applicable to operating plants and systems where operating data has been recorded over the entire operating range. The data-based systems are only accurate when applied to the same, or similar, operating conditions under which data was collected. When plant conditions or operations change significantly, the model must extrapolate outside the training space, and the results should not be trusted (Penha and Hines 2002).

The following types of solutions are found in this category:

- **Neural Nets**—computer systems that are able to learn the parametric relationships for operating regions that are presented to them during training. If the operating region moves outside the boundary of the training envelope, however, neural nets cannot be expected to give accurate results. The same is true for this entire category of solutions.
- **Nonlinear Geometric Representation**—a technique that attempts to derive a data distribution function based on normal operational parameter sets. Dissimilarities between the base case distribution and a threat case are quantified by nonlinear metrics to identify the existence of abnormalities.
- **Data-driven modeling**—an approach using group method of data handling. This method characterizes the measurements by nonlinear models whose generalization includes the use of rational functions of the measurements.
- **Multivariate State Estimation Technique (MSET)**—a statistical modeling technique that learns a high fidelity statistical model of an asset from a sample of normal operating data. The statistical model then provides an estimate of the signal in question and compares that estimate to the new observation from the asset. A comparison is performed

using a highly sensitive statistical process to indicate a process anomaly, sensor data quality problem, or equipment problem.

3.2.2.5 Stressor-Based D/P (the Integral Damage Model)

The premise of the stressor-based methodology is that by measuring stressor characteristics and correlating them to the observed degradation rate, a precursive physical relationship to component failure can be derived that will allow a much more meaningful and accurate projection of the remaining useful life (Jarrell 2002). Compared to the example portrayed in Fig. 3.2.1 of the trending technique, Figure 3.2.2 shows the expected result in narrowing the uncertainty by keying on the stressor itself and providing continuous feedback during the component lifetime from the stressor intensity.

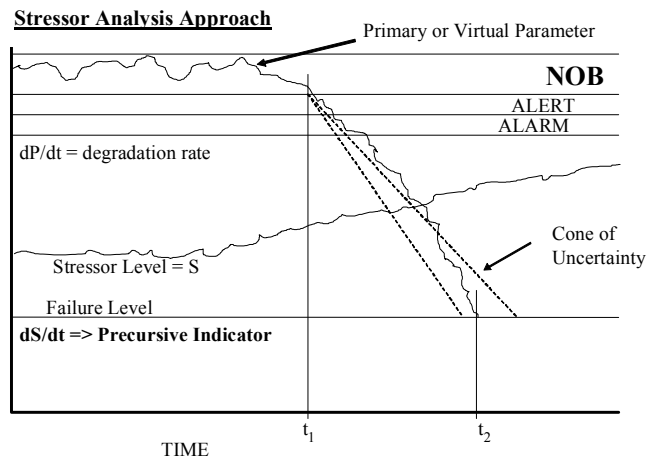


Fig. 3.2.2. Stressor measurement effect on prediction uncertainty.

The slope of the trended parameter gives a measure of the degradation rate of the performance. This is correlated through the rate of decline in the physical characteristics of the equipment. Integral damage techniques can then be used to correlate the previous, present, and projected condition of the equipment as a function of time.

3.2.2.6 Hybrid Systems

The combination of data-based and first-principle models are termed hybrid models. In these designs, first-principle models are developed and then appended with data-based models as normal mode data becomes available (Penha and Hines 2002). This method provides the robustness of first-principle models with the sensitivity of data-based models. This hybrid framework, although more complicated, has a very important advantage. Purely data-based systems are not reliable when the system moves into uncharted operating conditions that may result from configuration changes, new operating practices, or external factors such as unusual cooling water temperatures in condensers. By using the hybrid system, the predictions tend towards the first-principle model when new operating conditions are encountered and will additionally use the data-based models when in familiar operating conditions. Research on this topic is the least mature of current state-of-the-art work.

A movement toward total plant automation with operational status and diagnostic interaction has been achieved in advanced fossil plants and is at the cutting edge of nuclear plant I&C evolution

(Kim 2002). Few of even the fossil plants have, however, adopted the latest of these developing D/P technologies.

The control of a Generation IV reactor system will likely embody hybrid D/P systems as well as many of the other individual D/P methods discussed. Diagnostics will be integrated into control system logic to increase autonomous operation and lower operational risk and costs. The basis for diagnostic decisions may be model-based, derived from heuristics (i.e., rule-driven), or acquired from data mining of other systems.

3.2.3 Issues and Needs for Diagnostics and Prognostics Technology

Surveillances, diagnostics, and prognostics can be expected to assume an even more prominent role in future nuclear power plants, given the goals of minimizing the operations and maintenance staff, extending operational cycles, increasing maintenance intervals, and implementing multi-modular plants. The integration of diagnostics and controls for autonomous, intelligent plant control and information systems, and the transition to greater decision-making responsibility for the machine (i.e., the plant I&C systems) suggest the need for a well-founded understanding of the value added by D/P techniques and the reliability and accuracy of such methods. In addition, greater reliance on prognostics will prompt movement away from periodic manual tests and inspection and will provide a valuable decision-making asset during abnormal or emergency events. Therefore, it would seem reasonable to conduct research on expected near-term nuclear power applications of these emerging technologies [e.g., the techniques that are being developed under NERI and Nuclear Engineering Education Research (NEER)] and to monitor development in the technology through awareness of applications in other industries. In particular, methods for assessing the accuracy, stability, and reliability of diagnostic and prognostic techniques are appropriate candidates for near-term research.

This working group agreed upon a number of issues that they considered essential to the furthering of the D/P sciences. These fell into the following two main headings:

- Infrastructure needs
- Methods research needs

3.2.3.1 Infrastructure Needs

1. An adequate integral testing facility. While almost all of the DOE national laboratories and the major equipment suppliers have separate effects-testing apparatus, no real integrated test beds are available that would allow proof of combinations of the latest or emerging methodologies. Infrastructure and time-span aspects must be considered relating to active and passive components in reference to testing sensors and the relative time base of events (seconds versus years).

2. Definition of the man-machine authority split. Based on the reliability of future automated diagnostic and control systems, how much should the machine be allowed to control the reactor systems versus the operations staff? To a large extent, this will be dependent on the degree to which the software verification and validation (V&V) efforts are closely controlled and documented. The identified need is for close attention to the V&V programs for command-control software.

3. A well-defined protocol for documenting of process tomography. The use of inverse problem solutions depends totally on the adequacy of the characterization of the full set of design basis operational modes. Even the common expert systems approach would clearly benefit from a thorough understanding of a “normal” data set profile.

4. Integrate advanced D/P (and other) instrumentation into standard plant design criteria.

The results of current methods and developing technologies can be integrated into future designs and thus serve the data needs of future plants. This avoids the sometimes impossible task of retrofitting instruments into an established design envelope.

5. Increased sensor accuracy under adverse environmental conditions. Current instrumentation tends to be the least accurate under emergency conditions when it is needed most. Standards for sensor access are also needed to facilitate their calibration and replacement.

6. Field-hardened stressor-based sensors. These sensors need to be developed to allow deployment of accurate first-principle D/P methodologies.

7. Robust encrypted radio frequency (RF) tags. Tags need to be developed to ensure that a fault-tolerant and more easily retrofitted instrument communication system can be achieved.

8. Field-hardened distributed computing platforms for local D/P functional software. Computer-on-a-chip development would allow distributed D/P networks using health message communications rather than broadband data bursts.

3.2.3.2 Methods Research Needs

1. Uncertainty quantification for advanced D/P methods. This was identified as the highest priority concern. Historically, the NRC has been quite thorough in requiring error analyses for calculations such as criticality analysis where measurement errors in cross-sections are propagated through the calculations to the final result. Uncertainty inherent in advanced data-based models, however, is rarely discussed. For advanced D/P methods to be employed with confidence (i.e., can we trust the output?), we need to establish the uncertainty levels in the output and to recognize and incorporate them in our treatment of expected human-system interfaces and reactions. This issue is closely linked to the human-machine authority division issue.

2. Hybrid modeling. Opportunities through hybrid modeling are needed to overcome several observed problems in more conventional D/P methodologies. Data-driven techniques have been proven to be exquisitely sensitive to process abnormalities, but lack interpretive understanding and are often in error when applied outside the envelope of the training mode. First-principle approaches such as the integral damage model are continuously applicable and provide well-directed root cause analysis, but lack the ability to detect the onset of conditions that can lead to degradation and failure.

3. Stressor-based, first-principles D/P development. This development has been shown to be a reliable means of detecting and restoring design basis operation by identification of the specific degradation mechanism and off-nominal stressor(s). The completion of a full set of degradation correlations for critical components would provide effective accident prevention and, when necessary, would contribute to accident mitigation strategies.

4. Decoupling and recognizing the difference between control problems, process anomalies, and sensor drift. Control system malfunctions represent one of the most difficult problems to identify because they are often camouflaged by symptomatic system behavior and sensor fault scenarios to allow full validation the control system's effectiveness.

5. Data fusion and data mining techniques. The power industry should take advantage of these techniques from other process industries and apply them to nuclear operational data sets to

provide insights into failure D/P problems. D/P practices used in other process industries should be examined and reviewed for possible application to the nuclear industry.

6. Identification of minimum requirements for effective D/P. Sensing and monitoring methods must be evaluated during the design phase in order to minimize retrofitting.

3.2.4 Recommendations

3.2.4.1 Infrastructure Recommendation

1. An adequate integral testing facility.

Recommendation 1: Build a central user test facility that includes appropriately scaled major components and systems for testing advanced IC&HMI concepts and prototypes. The facility must contain an adequate physical representation of components to allow proof of concept for Generation II, III, and IV advanced systems. The facility placement should consider linkage with computational systems and simulators, allow true fault testing of equipment, be fully Internet accessible, and provide access to methods developers, vendors, and utilities. Particular attention should be paid to multiple-fault scenarios and data retrieval from control systems.

2. Definition of the man-machine authority split.

Recommendation 2: Establish a consensus standard through the IC&HMI (including NRC) and other standards groups for V&V certification of software systems.

3. A well-defined protocol for documenting of process tomography.

Recommendation 3: Create a dataset protocol standard for recording of operating mode data and the extent of mode envelope definition. The standard should treat data parametrics, minimum recording frequencies, and access specifications.

4. Integrate advanced D/P (and other) instrumentation into standard plant design criteria.

Recommendation 4: Through the IC&HMI group, organize a research instrumentation portfolio that targets the currently available (state-of-the-art) needs of the group in all six of the subgroup areas. Additional inputs should then be obtained from vendors, utilities, and EPRI. The finished portfolio would then be put on a permanently available web site for designer access.

5. Increased sensor accuracy under adverse environmental conditions.

Recommendation 5: Work with environmental qualification standards groups to extend concepts to tomorrow's instrumentation, including advanced smart sensors.

6. Field hardened stressor-based sensors.

Recommendation 6: Extend on-going research to catalog existing and envisioned sensor needs, and work with laboratory instrument development groups and instrument vendors to develop field deployable stressor instrumentation.

7. Robust encrypted radio frequency (RF) tags.

Recommendation 7: Take laboratory-developed RF tag devices to commercial vendors to field harden and enhance computational and transmission capability. Additionally, develop criteria for sensitivity testing for electromagnetic interferences (from motors, transmission lines, etc.) on RF systems, and for potential for RF tag influences on reactor protective systems.

8. Field-hardened distributed computing platforms for local D/P functional software.

Recommendation 8: Take laboratory-developed distributed computing devices to commercial vendors to miniaturize, field harden, and enhance computational and output capability.

3.2.4.2 Methods Research Recommendations

1. Uncertainty quantification for advanced D/P methods.

Recommendation 1: Establish a high priority initiative to quantify the uncertainty in each of the diverse existing methods and any future methods of D/P solution. Uncertainty in inputs, algorithm error propagation, operational mode definition, and the indeterminate nature of inverse problem solutions are specific topics to be covered under this initiative.

2. Hybrid modeling.

Recommendation 2: Conduct research into developing hybrid D/P models that contain the sensitivity of data-driven schemes and the robust root cause determination of the first-principles modeling. Use of both existing and emerging varieties of these program sets is encouraged to determine the most effective of the possible hybrid solutions.

3. Stressor-based, first principles D/P development.

Recommendation 3: Increase the research emphasis on first-principles methods to allow this emerging approach to mature as a solution set that identifies problem root causes. Reviewing and cataloging existing models must be incorporated in the emerging technology. The expected result is an accurate root cause identification process and a reliable solution to the vast majority of current and future generation reactor system failures. A coalition of university and national laboratory researchers is recommended.

4. Decoupling and recognizing the difference between control problems, process anomalies, and sensor drift.

Recommendation 4: Solicit projects aimed at uniquely identifying the instrumentation set and detection methodology to uncover control system specific malfunctions. After the proof of concept has been demonstrated, the method must then be subjected to independent control, process, and sensor fault scenarios to fully validate its effectiveness.

5. Data fusion and data mining techniques.

Recommendation 5: Perform directed research that initiates a literature search of non-nuclear D/P methods and then selects potential applications based on criteria specific to the nuclear community. This best practices guide would then be used to direct future research investigations.

6. Identification of minimum requirements for effective D/P.

Recommendation 6: Extend on-going research to catalog existing and envisioned sensor needs, work with laboratory instrument development groups and instrument vendors to develop field deployable stressor instrumentation.

3.2.5 References for Diagnostics and Prognostics

- Bond et al. 2000. "On-Line Intelligent Self-Diagnostic Monitoring for Next Generation Nuclear Power Plants," Proceedings of the Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies 2000. ANS CD.
- Bond, L.J. 1999. "Predictive Engineering for Aging Infrastructure" (Plenary Paper), in *Nondestructive Evaluation of Utilities and Pipelines III*, Ed. W.G. Reuter, Proceedings SPIE, Vol. 3588, pp 2–13.
- Edwards, R. M. 2002. "Monitoring and Control Research Using a University Reactor and SBWR Test-Loop," IC&HMI Presentation, May 15.
- Esselman, T.C., M.A. Eissa, and W.J. McBrine. 1998. "Structural Condition Monitoring in a Life-Cycle Management Program," *Nuclear Engineering and Design*, Vol. 181 pp 163–173.
- Hadden, G.D., P. Bergstrom, T. Samad, B.H. Bennett, G.J. Vachtsevanos, and J. Van Dyke. 2000. "Application Challenges: System Health Management for Complex Systems." Parallel and Distributed Processing Proceedings. *Lecture Notes in Computer Science*, Vol.1800 pp 784–791.
- Jarrell, D.B. and R.D. Stratton. 1991. "The Effects of Root Cause Analysis on the Utility Resource Balance," Advances in Industrial Ergonomics and Safety III, Taylor and Francis.
- Jarrell, D.B., L.J.Bond, and D.R. Sisk. 2002. "A Foundation for Stressor-Based Prognostics for Next Generation Systems," Proceedings of the ASME ICONE10, Topical on Nuclear Engineering, April.
- Kaistha, K. and B.R. Upadhyaya. 2001. "Incipient Fault Detection and Isolation of Field Devices in Nuclear Power Systems Using Principal Component Analysis," *Nuclear Technology*, Vol. 136, pp. 221–230, November.
- Kim, D S, et al. 2002. "Design Improvement on Ulchin Nuclear Power Plant Units 5 and 6," Proceedings of the ANS Embedded Topical on Advanced Nuclear Power Plants, June.
- Kramer, M.A. and B.L. Palowitch.1987. "A Rule-Based Approach to Fault Diagnosis Using the Signed Directed Graph," *AIChE Journal*, Vol. 33, No. 7, pp. 1067–1078, July 1.
- Montmain, J. and S. Gentil. 2000. "Dynamic Causal Model Diagnostic Reasoning for Online Technical Process Supervision," *Automatica*, Vol. 36, pp. 1137–1152.
- Penha, R. L. and J. W. Hines. 2002. "Hybrid System Modeling for Process Diagnostics," Proceeding of the Maintenance And Reliability Conference (MARCON).
- Upadhyaya, B.R. 2002. "I&C and HMI Workshop: Diagnostics and Prognostics," IC&HMI Presentation, May 15
- Upadhyaya, B.R., B. Lu, and K. Zhao. 2002. "Equipment Monitoring During Transients and Multiple Fault Conditions," Proceedings of MARCON 2002, May.

- Vedam, H. and V. Venkatasubramanian. 1995. "PCA-SDG (Signed Directed Graph) based Process Monitoring and Fault Diagnosis," *Applications of Artificial Intelligence*, Vol. 8, pp. 689–701.
- Walke, D. 1998. "Advances in Engine Management and Diagnostics," *Quarry Management*, February, pp 19–22.
- Waterman, D.A. 1986. *A Guide to Expert Systems*, Addison-Wesley.

3.3 COMPUTATIONAL METHODS

3.3.1 Session Participants and Goals

3.3.1.1 Participants

Ray Brittain, Oak Ridge National Laboratory
Mo Jamshidi, University of New Mexico
Nihal Kececi, University of Maryland
Jesse Poore, University of Tennessee
John Scott, Lawrence Livermore National Laboratory
Carol Smidts, University of Maryland
Eric Thornsby, U.S. Nuclear Regulatory Commission
Lefteri Tsoukalas, Purdue University
Richard Wood, Oak Ridge National Laboratory

3.3.1.2 Goals

This session addressed research issues related to control and decision methods and high-integrity software approaches. The goal of this session was to identify research needs to enable high-integrity software systems that can provide the control, decision, and protection functions required to support nearly-autonomous operation of advanced nuclear plants over extended-operation cycles under a full operational regime.

3.3.2 Overview of the State of Computational Methods Technology

The discussions by the Working Group during this session addressed challenges posed by the aggressive operational and economic goals set for advanced nuclear plants that are likely to require innovative I&C technology and changes in the traditional concept of operations. These challenges include (1) automation of control that can accommodate complex operational conditions (especially those posed by multiunit plants with integrated process systems) and adjust in response to changing or degrading conditions (assuming a trend toward reduced maintenance staff and extended intervals between maintenance); (2) assumption of significant decision responsibilities by the “machine”; and (3) adoption or adaptation of software engineering/reliability estimation techniques that are necessary to enable development and assessment of high-integrity software-based decision and control systems.

The operation of a system or process is managed through the interaction of humans or equipment with field devices (i.e., actuators) that can affect the process (i.e., control). The command for a specific action is initiated by either manual input or automatic control action (or some combination of both) based on information about the state of the system or process (e.g., measurements, diagnostics, constraints, procedures). For automatic control, the command or control action is the result of calculations or logic that is based on process measurements and accomplished by control algorithms implemented in hardware or software. For automatic control, no operator intervention is required, although the automatic control function can be switched out (i.e., over-ridden) to permit manual control.

In traditional control systems, the decision making (i.e., the choice among valid solutions or options) is left to the human. Elements of the decision process, either during design or operation, include determination of the control strategy (i.e., goals, key variables, available actuators) to be employed, establishment of the acceptable range of actions, and the coordination among individual control loops. In contrast to automatic control, autonomous control involves the combination of control and decision capabilities without required human intervention.

The range of control and decision capabilities is a key element of this technology focus area. In the nuclear power industry, single-input, single-output classical control has been the primary means of automating individual control loops. The use of multivariate control, such as three-element controllers for steam generators, has been employed in some cases. In a few cases, effort was made to coordinate the action of individual control loops based on an overall control goal. The application of other techniques to nuclear power control issues has been primarily the domain of universities and national laboratories. Some of the techniques employed in controls research for both power and research reactors include adaptive robust control for the Experimental Breeder Reactor II, fuzzy control, H-infinity control and genetic algorithm-based control for steam generators, neural network control for power distribution in a reactor core, supervisory control for multi-modular advanced liquid-metal reactor (ALMR). Current control systems marketed for the nuclear power industry are based on microprocessors or programmable logic controllers (PLCs). Most of these systems offer control application building software that contains basic control blocks that can be graphically configured into a control algorithm. These systems offer classical control modules as well as model-based control options. Several nuclear power plants have initiated control system upgrades as part of the plant life extension effort (Taylor 2000; Kim 2002).

The most significant change that is expected in control system development for future nuclear power plants may be the transfer of more and more of the decision-making responsibility to the I&C systems. Given the staffing and operational cycle goals of long-term deployment reactor concepts and the prospect of multi-modular plants with integrated process systems and/or control rooms, the move to highly automated control and information systems seems inevitable. Therefore, consideration was given to the capabilities and reliability of autonomous control systems.

This leads to the second key element of this technology focus area, high-integrity software. As a result of the continuously expanding uses of software in every aspect of life, many highly critical engineered systems have begun using software-based digital systems. These include control of passenger aircraft, control of many kinds of military hardware from ship navigation to targeting of smart bombs, control of the national electrical grid, and control of many forms of diagnostic and therapeutic medical devices. Because of the high consequences of failure of these systems, the need for high-integrity software has increased significantly. From the perspective of its use in nuclear power plants, the on-going plans by several utilities to retrofit reactor protection system instrumentation and control systems with software-based digital systems, movement toward the increasing use of commercial-off-the-shelf software-based equipment, and the likelihood of highly autonomous control systems for future plants indicate the need for new methods for developing and assessing very high-reliability, high-quality software.

The nuclear industry requirements for computer-based safety systems are identified in Annex E of IEEE Std. 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." IEEE 7-4.3.2 requires that digital safety systems be designed, fabricated, installed, and tested to quality standards commensurate with the importance of the safety functions to be performed. Industry practice requires establishing a software life-cycle process at the beginning of safety system development. The software developer may be the licensee, the vendor, a company working on behalf of either, or a commercial software development company. Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE 1074, "Standard for Developing Software Life Cycle Processes," provides guidance for the implementation of a software life cycle plan. However, developers of software for nuclear applications generally still use traditional software development methods. In assessing research

needs the aspects of high integrity software that were considered include software development methods, software assessment methods, and software reliability.

3.3.3 Issues and Needs for Computational Methods Technology

This working group identified several technical areas within the field of computational methods that pose research issues that should be addressed to facilitate the realization of future nuclear power development. These topics include control and decision methods, software quality assurance, digital system risk assessment, and commercial-off-the-shelf (COTS) software. These technical areas are discussed below with an identification of specific research needs.

3.3.3.1 Control and Decision Methods

Future nuclear plants are likely to rely on increasing degrees of automation and self-monitoring to support reduced staffing, optimize performance, and minimize scheduled maintenance. In addition, the 60 year or more life time for future plants will probably involve several upgrades of computing and control equipment with the expansion or improvement of functional capabilities. Therefore, a coordinated effort should be made to establish a control system architectural framework (i.e., hierarchical functionally) that can facilitate the integration of control, decision, and diagnostics. This framework should also incorporate captured expertise and provide flexibility and expandability for growth during the plant life cycle. In addition, advanced control concepts should be demonstrated to provide the foundation for intelligent (i.e., self diagnosing, self correcting, self validating) and autonomous (increased responsibility/authority, higher functionality) control. A specific subject that is ripe for such research is control of multi-modular nuclear plant implementations. Projects investigating the unique control issues arising from the dynamic behavior of units with shared process systems could provide the key developments to achieve the goal of a comprehensive control system architectural framework.

3.3.3.2 Software Quality Assurance

The current reliance on qualitative indication of software quality often leads to high development and implementation costs for safety-related digital systems with no direct evidence that the software will perform its intended function on demand under every circumstance. While there is much research in the field of software engineering, there has not been a consensus developed on quantitative methods for software quality estimation. Given the unique safety considerations for the nuclear industry, it seems clear that software engineering practices should be investigated and employed and comprehensive systematic methods for quality determination of software should be developed and demonstrated. The first and often most crucial step in developing a software-based system is to define the necessary and complete set of system requirements and correctly translate those requirements into the associated software specifications. Systematic approaches are needed for developing and evaluating functional requirements and software specification. Experience has shown that many software errors can be traced to inadequate or misinterpreted requirements. To address this potential weakness, a set of quality attributes characterizing requirements correctness should be defined, techniques for expressing requirements in forms (e.g., mathematical, graphical) that are more amenable to analysis and review should be developed, and systematic approaches for the translation of requirements into specifications (e.g., sequence-based specification) should be demonstrated. A second needed element related to the quality assurance issue is to promote the use of sound software engineering practices for the generation of software-based systems. Examples of such practices include the clean room approach (Prowell 1999), the trace assertion method (Janicki and Sekerinski 2002), the Goal/Question/Metric (GQM)/Quality Improvement Paradigm (QIP) approach (Basili 2002), and the personal software process (PSP) and team software process (TSP) methods (Humphrey 2002). The specific research need in this area for the nuclear power industry is to examine the leading software development practices to characterize their capabilities and determine their suitability for adoption by the nuclear power community. Benchmark projects applied to nuclear power safety-related systems of moderate

complexity could contribute to addressing this need. As a third element of addressing software quality assurance, consensus among practitioners within the nuclear industry should be established for a complete set of quality attributes with related measurement approaches. Continuation and expansion of recent studies sponsored by the NRC can contribute to this effort. Finally, a fourth element of research for addressing the issue of software quality assurance is the establishment of manageable approaches to high-integrity software validation testing. Model-based statistical testing has demonstrated success in the computing industry and should be investigated through a nuclear power demonstration. In addition, fault seeding approaches and testing programs using massively parallel computers (based on inexpensive personal computers) have shown promise and should be developed further.

3.3.3.4 Risk Assessment for Digital Systems

The move to a risk-informed regulatory environment is constrained by uncertainties in how to adequately characterize the risk associated with digital I&C systems. This issue highlights the need for comprehensive, systematic methods for determining the risk of digital systems. To attain this goal, reliability modeling capabilities for hardware, software, and system interfaces should be developed and demonstrated; reliability databases for software-based systems are also needed (i.e., relevant data characteristics need to be determined and mechanisms for capturing data should be developed). To facilitate effective evaluation of risk, a dynamic reliability environment should be developed to provide tools for automating/enhancing reliability modeling and risk assessment. Finally, software categorization should be investigated to determine the capability to establish software classes for quantification of risk to address software configuration, reuse, or revalidation after modification.

3.3.3.5 Commercial Off-the-Shelf (COTS) Software

Economic and market forces are driving the nuclear power industry toward an increased reliance on COTS. Thus, a need exists for methods to determine the quality of a digital system composed of integrated software elements that may include pre-existing code of incomplete or unknown pedigree. Such research should provide product evaluation tools that address methods for determining the minimum requirements needed for quality assurance while considering the application's complexity and domain. In addition, research is needed to investigate the scalability of the software life-cycle process based on the simplicity of application and integration of prequalified components.

3.3.3.6 Software Fault Handling

Software fault tolerance is a key issue in developing dependable high-integrity, software-based systems. Approaches for addressing faults include fault avoidance, fault removal, fault tolerance, and fault prediction. Fault avoidance approaches include the application of formal methods, object-oriented coding, and software reuse. Formal inspection, data flow testing, and fault insertion (e.g., software-based and state-based) are examples of fault removal techniques. Fault tolerance can be promoted through design diversity or by software implemented fault tolerance (SWIFT) methods such as error detection, error recovery, and data recovery. Reliability modeling, reliability data collection, operation profile identification, and rare event prediction are means of performing fault forecasting. There is on-going research sponsored in part by the NRC to demonstrate software-based fault tolerant techniques for a nuclear power application. Research of this kind should be continued and expanded to promote development of methods and approaches that are appropriate for nuclear safety-related usage and to demonstrate their effectiveness in nuclear power applications.

3.3.3.7 Simulation Capabilities for On-line Applications

With the expectation that intelligent, autonomous control will be employed in future plants, the increasing use of fast, detailed plant and component simulation models for control and

diagnostics/prognostics development and testing is likely. Although advanced simulation techniques modeling research in and of its self is not a high-priority subject for nuclear power, modeling development and simulation applications need to be considered as a part of other, more broadly focused research projects. Examples of research activities that can help establish the uses of simulation to support plant management and identify application limitations are prediction/consequence determination, diagnosis of condition or state identification, stress estimation, and decision support (e.g., temporal limits for event response, operational regime trajectory warnings).

3.3.3.8 Redundancy and Diversity for Digital Systems

The traditional approach for providing the necessary level of safety assurance in safety-related I&C applications at nuclear power plants has included redundancy and diversity. In the digital realm, some uncertainty exists concerning exactly what satisfies those conditions and what value is derived for various approaches. A clear definition of diversity and redundancy is needed for digital systems. Research should address the design aspects (How much and what kind is needed?) and the evaluation aspects (How much value should be attributed to different approaches and what dependencies exist?).

3.3.4 Recommendations

The research needs described previously can serve as the basis for numerous individual projects directed toward the stated goals for high-integrity, software-based command and control systems in future nuclear power plants. However, it is the consensus of the working group that the most effective means for facilitating that research and achieving the desired capabilities is to develop a virtual control system test bed. Such a test bed could be composed of distributed research user facilities with coordinated physical and/or networked access. The user facilities should be based on existing research resources (e.g., computer labs, simulators/models, process test loops, control hardware, network interoperability test beds, software testing lab) and new test bed elements that are developed as part of NERI, INERI, NP2010, or Gen IV projects. This working group recommends that existing research capabilities be surveyed, an advisory committee to coordinate interaction and access be established, and research projects, based on the described research needs, be funded to contribute any missing elements of the overall test bed capability.

3.3.5 References for Computational Methods

Basili 2002. <http://www.cs.umd.edu/~basili/>.

Humphrey 2002. *Winning with Software: an Executive Strategy*. Addison-Wesley. Reading, MA.

Janicki and Sekerinski 2001. "Foundations of the Trace Assertion Method of Module Interface Specification," *IEEE Transactions on Software Engineering*. Vol. 27, No. 7, July.

Kim, D.S., et al. 2002. "Design Improvement on Ulchin Nuclear Power Plant Units 5 and 6," *Proceedings of the ANS Embedded Topical on Advanced Nuclear Power Plants*, June.

Prowell, et al. 1999. *Cleanroom Software Engineering*. SEI series in software engineering. Addison-Wesley. Reading, MA.

Taylor 2000. "Oconee Nuclear Station Integrated Control System (ICS) Replacement Project," *Proceedings of the Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies 2000*. ANS CD.

3.4 COMPUTING AND COMMUNICATIONS ARCHITECTURES

3.4.1 Session Participants and Goals

3.4.1.1 Participants

Christina Antonescu, Nuclear Regulatory Commission

Bruce Cook, Westinghouse

Paul Ewing, Oak Ridge National Laboratory

Doug Hill, MPR

Jim Keiper, Foxboro

Kang Lee, National Institute of Science and Technology

Paul Loeser, Nuclear Regulatory Commission

Joe Naser, Electric Power Research Institute

Dinesh Taneja, Bechtel Power

Kobus Janse Van Rensburg, PBMR (Pty) Ltd

Reed Wiegler, CANUS Corporation

Ted Quinn, General Atomics

3.4.1.2 Goals

The goal for this section is to provide an overview of the state of the art and challenges for the next three to five years in computing and communications architecture for advanced nuclear plants. It addresses the following major technical areas in computing and communications architecture:

- Functional configuration and distributed resource management
- Data communications
- Information management (e.g., plant “language” or ontology, security, access)

3.4.2 Overview of the State of Computing and Communications Architectures Technology

Plant monitoring and display systems monitor plant variables and provide data to other I&C systems and to the plant operators for use in controlling the operation of the plant. Typical examples include systems that monitor and display the status of the fire protection system, fluid temperatures, and pressures. These systems also normally provide visual and audible alarms at various control stations, particularly the main control room, that notify operators of trends or particular values requiring action by the operators to avert an actual problem or emergency. Usually operators follow formal procedures when an alarm or notification occurs; these procedures use alarm setpoint and required responses that are coordinated to give the operator adequate time to take action. Typically, the response times are on the order of minutes; or if inadequate time exists, an automatic response is provided.

Figure 3.4.1 illustrates a modern digital computing and communication architecture system. Blocks on the lower left represent the distributed control systems. These systems regulate plant conditions during startup, power operation, and shutdown. They normally operate in a regulating mode to maintain plant systems and components within their operating ranges.

As seen in Figure 3.4.1, redundant data buses are included for the control and monitoring architecture. These data buses transport the large amounts of information typically handled in large generating stations. Using data buses reduces and simplifies plant wiring and consequently reduces requirements for managing and maintaining wiring configuration. Redundancy and separation (including different routing) provides increased data bus reliability. In this manner, reliable communications can be provided for the large number of information data points. These system-level modules also provide real-time control functions. The lower right side of Fig. 3.4.1

shows the independent (safety) protection systems. These systems detect system failures and isolate or shut down failed components to protect the plant and public health. This type of system normally uses multiple channels in a voting scheme to trigger the isolation or shutdown action. A typical scheme uses a two-out-of-four logic.

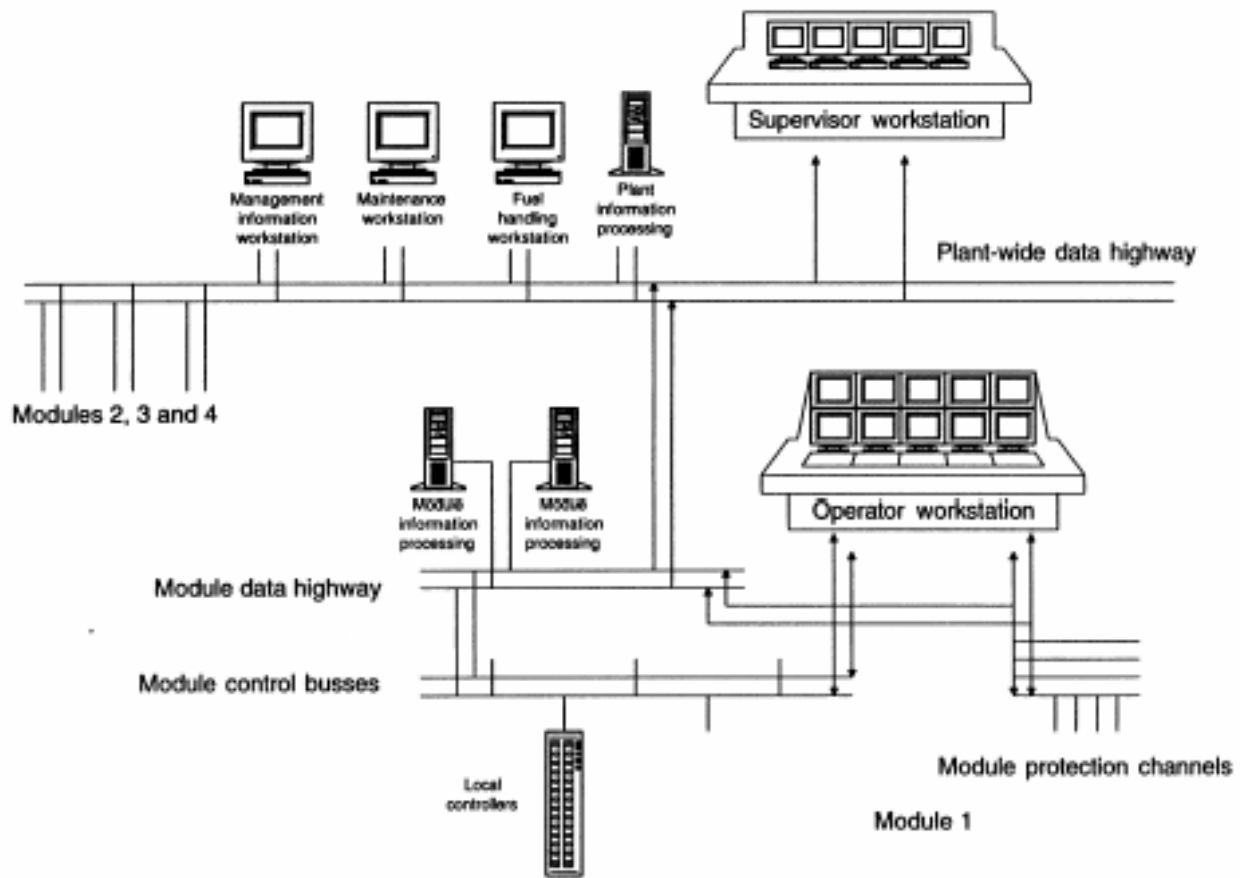


Fig. 3.4.1. Advanced U.S. nuclear plant design communications and control architecture

Figure 3.4.1 also shows the point-to-point data links in the protection system that provide for more deterministic and predictable data communications for the fewer data points that are normally needed in safety system architecture. An independent manual trip normally bypasses all the microprocessor-based trips.

In the United States, the advanced reactor designs being developed incorporate all-digital systems intended to utilize and exploit the new technology. New reactor designs also feature enhanced human-machine interfaces such as the more versatile displays with integrated process information. These features and other features make the advanced plants simpler and safer. Certification of three of the designs has been accomplished under the provisions of 10 CFR 50.52.

The major challenges to the introduction of these new systems include the following subjects:

- Uncertainty inherent in introduction of new technologies
- Shift of existing technology base from analog experience
- Technical problems identified from some applications of digital I&C for upgrades to existing U.S. plants and in new foreign plants
- Difficulty in first-time digital applications going thru the NRC licensing process

Recent experience with large-scale, fully integrated digital I&C systems at nuclear power plants has also had its difficulties. Problems, apparently related to system aspects, have caused substantial delays and increased costs. In addition, increased use of open systems, in which multiple vendors provide components, requires assurances that these components successfully interact. Open systems are used because they foster competition and standardization and avoid dependence on single suppliers. However, the presence of multiple vendors may make successfully dealing with system aspects more difficult because of the increased number of interfaces.

Several new nuclear plants have been completed overseas in the past few years, using completely digital-based systems and which represent significant digital I&C integration efforts. These plants are the United Kingdom's Sizewell B, France's Chooz-B plant, Canada's Darlington plant and Japan's Kashiwazaka-Kariwa Units K-6 and K-7. Sizewell B includes a distributed digital control system for control and data acquisition that is part of a product family that has been used extensively in process control applications, including fossil-fired generating plants. It also includes elements of a nuclear safety-grade product family for protection that has been used in some nuclear applications. Redundancy is provided at all levels, including dual redundant conductors for data buses and two diverse protection systems. Hard-wired controls and instruments provide backup for computer-based systems. The French Chooz-B design uses a three-level architecture. The Canadian program uses digital control and monitoring because significant computational capability is required to maintain adequate neutron flux distribution and stability for the Darlington plant. The Japanese design for K-6 and K-7 meet the bulk of the requirements for the equivalent U.S. advanced boiling water reactor plant that has completed design certification. All of these plants are now producing power on the grid. Several years of experience exists with these large systems.

Digital computing and communication architectures are also used in many other safety-critical industries such as aerospace and the chemical industry. Experts from these industries will also be sought to address lessons learned in the applications of advanced I&C to their industries.

This industry experience is closely linked to the man-machine interface issue and challenges of introducing new control room architecture and plantwide control and monitoring operations.

3.4.3 Issues and Needs for Computing and Communications Architectures Technology

The following analysis topics were addressed as part of the Group IV working group discussions (not in order of priority). Each issue is discussed in the following section. Specific recommendations on how to address each issue are in the following section.

- Cyber security
- Performance issues
- Wireless systems
- Complexity
- Risk-informed design and operation
- Industry standards issues
- Autonomous operation
- Life-cycle management

3.4.3.1 Cyber Security

In the past few years, and especially since 9/11/01, cyber security has been a major issue for nuclear energy and includes the following areas for consideration:

- Protection against internal or external threats (both malicious and inadvertent)
- Hacker tolerance and unauthorized access

Example: A dial-up network has potential to allow an unauthorized person have access to the plant and thus allow unauthorized control changes in the plant.

Example: Wireless communication could lead to denial of service through jamming.

3.4.3.2 Performance Issues

Overall performance of instrumentation systems is a critical area and includes the following related but diverse areas:

1. Failure modes

- Fault tolerance/fault recovery
- Intermittent failures—processor resets
- Rules for operation under loss of communication system/display
- Data highway failure modes and probabilities
- Common cause failures of communications network

2. Environment

- Wireless reliability
- Operation in harsh environments
- Radiation sensitivity
- EMI/RFI (high frequency)

3. Performance

- Rules for information exchange from nonsafety to safety
- Role of distributed control vs. smart sensors
- Localized data processing

- Operations under abnormal and degraded conditions
- Distributed computing (Internet, intranet, subnet)
- Redundancy, diversity
- Real-time performance
- Appropriate time response

4. Software reliability quantification

3.4.3.3 Complexity

The following issues are related to complexity:

- Rules for exchange of information from nonsafety to safety
- Multi-module–single system vs. multi system applications
- Wrong module operation and maintenance issue
- Integration vs. standardization (use of multivendor equip)
- Localized data processing
- Learning curve
- Embedded software and smart sensors

3.4.3.4 Risk-Informed Design and Operation

The following issues are related to risk-informed design and operation and were discussed at the sessions:

- Role in Generation III and Generation IV designs
- Prioritization of activities–safety system first
- Risk issues–safety and financial
- Consequences of failures
- Relationships between architectural and risk contributors
- Software reliability

3.4.3.5 Industry Standards

The following issues were discussed and addressed, related to industry standards:

- Guidance for autonomous systems
- Standards for computing and communication architecture
- Take advantage of other industries' experience and technology

3.4.3.6 Autonomous Operation

The following issues were addressed relative to autonomous operation:

- Multimodule/multisystem operation
- Guideline for autonomous control (diffuse control)
- Multimodule remote control
- Distributed computing (Internet/intranet/subnet)
- Network design for control of autonomous processes

3.4.3.7 Life-Cycle Management

The following life-cycle management issues were addressed as part of our sessions:

- Expandable/flexible architecture
- Life cycle management–I&C life cycle vs. plant life cycle
- Coping with different construction phases–multimodular construction/operation sequencing
- Sufficient bandwidth to last over life cycle

- Cost effective design, modeling and simulation tools
- Operation and maintenance as a function of life cycle

3.4.4 Recommendations

1. Cyber Security

Recommendation 1: Develop guidance on how to handle internal or external threats and hackers.

2 Performance Issues

Recommendation 2:

- Authorize research into digital failure modes and probabilities as input to overall plant PRA.
- Identify potential vulnerabilities of computing and communication systems in the presence of environmental stressors, including predicted Generation IV environment.
- Research radiation hardened I&C communication systems/smart sensors.
- Provide design guidance to achieve target system performance in the context of nuclear regulation.
- Software reliability—follow and complement industry software reliability quantification research.

3. Complexity

Recommendation 3: Develop interoperability test bed and new simulation tools for evaluation of smart sensors, networks, and training.

4. Risk-Informed Design and Operation

Recommendation 4: Investigate new ways to look at architecture division of systems based on risk-informed principles (with Group VI).

5. Industry Standards Issues

Recommendation 5:

- Evaluate applicability of other industries' standards and technologies for communication and networking to achieve safety and performance goals
- Support open communication standards that enhance network efficiency. (Example: PBMR application of IEC 61508)
- Evaluate need for mapping between IEEE 1451 and field bus protocols

6. Autonomous Operation

Recommendation 6: Develop guidance for autonomous system network design, management, and control.

7. Life-Cycle Management

Recommendation 7:

- Provide guidance for design and maintenance of computing and communication systems over design lifetime to minimize impact of digital system obsolescence.
- Develop criteria to assist in decision process.

3.5 HUMAN-SYSTEM INTERACTIONS

3.5.1 Session Participants and Goals

3.5.1.1 Participants

Dennis Bley, Buttonwood Consulting
Joseph DeBor, Aeroflex Altair Cybernetics
Richard Eckenrode, Nuclear Regulatory Commission
Bruce Hallbert, Idaho National Engineering and Environmental Laboratory
Conny Holmström, Halden Reactor Project
Jacques Hugo, PBMR Ltd
John O'Hara, Brookhaven National Laboratory
Jay Persensky, Nuclear Regulatory Commission

3.5.1.2 Goals

To meet these goals of Generation IV plant design and to take full advantage of digital I&C and computer technology developments, new and innovative approaches to the human interaction with the plant are needed. The goal of the working group was to define the research needed upon which advances in the integration of personnel into plant design can be made.

3.5.2 Overview of the State of Human-System Interactions Technology

Generation III plants are essentially simplified and computerized version of their predecessors. While this is an improvement over earlier designs, it did not represent a fundamental change in approach. For example, the crew organizational structure and their roles and responsibilities are the same as for older plants. The control room designs provide human-system interfaces (HSIs) that are primarily based on digital technology, such as software-based controls and computerized procedures. The displays resemble conventional control boards showing plant systems as mimic displays. Little advanced graphic display technology is used to provide enhanced displays that could support disturbance analysis and improved situation awareness. Also, little or no use of intelligent systems exists in early designs. In sum, Generation III nuclear plants provided computerization, but do not tap the full strength of digital I&C and computer systems. The vision for Generation IV plant designs includes ambitious goals of improved economic competitiveness, reliability, and safety.

This group followed a top-down approach that began with a consideration of Generation IV goals. Advances needed to meet these goals were identified as was the research needed to address them. The group also considered whether the research tools currently available were sufficient to conduct the identified research. Where they were deemed to be inadequate, R&D infrastructure needs were identified. Figure 3.5.1 provides an illustration of this approach.

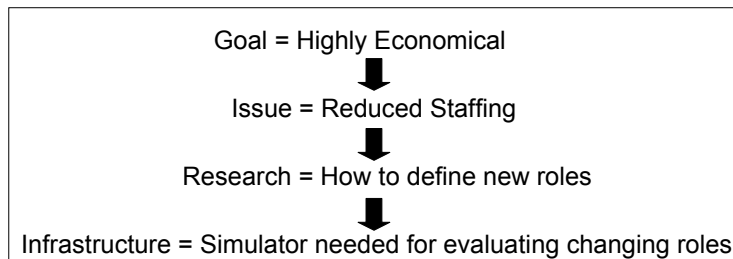


Fig. 3.5.1. Top-down approach evaluating human-system interaction research needs.

3.5.3 Issues and Needs for Human-System Interactions Technology

The working group concluded that to achieve Generation IV goals, significant changes in the concept of operations will be needed, including changes to the relative roles of human and system resources in plant monitoring and control, the design of HSI, and the tools provided for personnel to plan, interact with each other, and conduct their tasks. An important aspect of human-system interaction research should be on better use of the tremendous advances in I&C (e.g., smart sensing, automated monitoring and diagnostic systems, and computational simulations) that will emerge as Generation IV technology develops. These research needs are discussed in four sections below, addressing:

- Concept of operations
- Advanced human system interfaces (HSIs)
- Knowledge engineering and computer-supported cooperative work
- Human-system interaction R&D infrastructure

It should be noted that these topics are not mutually exclusive.

3.5.3.1 Concept of Operations

A concept of operations is a broad topic that can be broken down into the following key elements:

- Functional staffing models
- Plant automation
- Training and qualifications.

Functional Staffing Models

Current plants have a large number of on-site personnel organized into functional groups, including operations, maintenance, engineering, administration, security. From an operations perspective, a plant is controlled by a crew which includes numerous individuals in the control room and in the plant. Shift staffing and training of plant personnel is a very costly aspect of plant operations. Generation IV reactor technology will be fundamentally different than the current fleet of LWRs and will require a new vision of how to operate and staff the plant. The process of developing the best vision for operating the plant should be based in technology and treated as an integral aspect of design. After this overall operational vision is identified, the evolutionary path to achieving the selected operational model should be identified.

Some candidate models are

- onsite, multiperson crew for one reactor (current operational model);
- onsite, multiperson crew for multiple reactors;
- onsite, reduced staff with an individual for one reactor;
- onsite, reduced staff with an individual for multiple reactors;
- decentralized functional groups; and
- fully remote operations.

While many models are possible, economic and safety objectives should take priority. Once identified, the model becomes a design driver for levels of automation, staffing, and qualifications, HSI design, personnel training, etc. One example of functional design is a decentralized functional groups model. In this example, the plant (consisting of multiple reactor modules) would be staffed with a very small number of onsite personnel. Unlike today's operational environment, the on-site crew would be largely made up of technicians who keep an

eye on the highly automated operation and occasionally perform a minor operations or maintenance task. This crew would have minimal training. Responsibly for all but normal operations would be handled by off-site specialists who either come to the plant when needed (for maintenance, for example) or perform their tasks remotely. For example, very highly qualified crisis team would assume control (possibly from a remote location) when a disturbance occurs. Because of the low probability of such an accident, this team would be available for many reactor sites. This model supports Generation IV economic goals because of the greatly reduced staffing and training burdens. It will also support safety goals because this highly trained team would be responsible for nothing but handling crises, thus their level of expertise and ability to use analysis tools would be superior to what could be attained when a single crew has to handle everything (today's model).

While this is only an example, operational models have to be identified, tested, and designed into the Generation IV plant. Research is needed to define and evaluated alternative models using modeling techniques and simulation facilities. The research should not only define the endpoint vision for Generation IV plants but also the evolutionary strategy to get there.

Plant Automation

A proper mix of human and automatic systems is needed to maximize overall human-system efficiency, reliability, and safety for the selected models of operations. Historically, we think of automation with respect to plant control functions. For Generation IV, we need to think more broadly and look for opportunities to introduce automation to support all human cognitive functions, including monitoring, disturbance detection, situation assessment, response planning, and response execution. An optimum balance of human and automation resources will result in a "joint cognitive system" for plant monitoring and control. This type of user-friendly and cooperative automation will make Generation IV advances possible and will require a significant change from current approaches.

Research is needed to develop a technical basis for allocating functions to system or human resources, such as a parametric model for adaptive automation. The research elements include

- establishing the relationship between the level of automation required by functional staffing concepts ;
- determining the level of information required to keep the operator informed of automation status;
- developing methods to minimize the negative effects of automation on personnel, such as operator's loss of situation awareness, loss of vigilance, and skills degradation; and
- using strategies for transitioning from automatic to manual control.

Tools and techniques to perform function and task analyses need to be developed that can be used to evaluate staffing needs. Such analytical approaches for evaluating staffing requirements for complex systems have been evolving over the past few years. Human behavioral modeling techniques, such as task network modeling and discrete event simulation, have been developed and tested by the U.S. Army and Navy, and some of these techniques have been accredited by the U.S. Department of Defense for use in HFE analyses during system design and engineering. These human behavioral modeling techniques and tools need to be developed or adapted to determine staffing needs for advanced reactors. The use of such analytical models could enhance the efficiency and effectiveness of the plants while ensuring safe operations.

Training and Qualifications

Research is needed to define the training and qualification requirements for plant personnel based on the functional staffing models selected. Qualifications are generally based not only on training but also education and experience. The knowledge and abilities required of different staffing functions need to be defined. Training models need to change to provide for distributed training, embedded training, and virtual reality.

3.5.3.2 Advanced Human System Interfaces

While advanced HSIs will be applied plantwide and across the organization, the following discussion focuses on operations and maintenance functions. Relative to current Generation III HSIs, we envision Generation IV HSIs to be

- more intelligent,
- more integrated,
- more directly meaningful, and
- less difficult to use.

The major design issue is the development of HSIs in the context of reduced staff, changes to personnel role, and multiple unit operations. A challenge is to develop an interface through which plant personnel can obtain information effortlessly, when and where they need it, and in an immediately understandable form with no need to translate the presented data to obtain the information needed. The interface should be tolerant to personnel errors when they occur (i.e., minimize the chances that errors will occur and ensure error detection and recovery when they do occur). Research will be needed to develop a fully integrated control room supporting all operational and maintenance activities by a combination of crew members, intelligent agents, and automatic systems. Some of the components of such an interface include (1) higher-level, more meaningful displays, (2) integration and information hierarchies, and (3) low workload navigation and interface management. New interface technologies (e.g., voice recognition, real-time simulation, and advanced methods of presenting displays of complicated information—virtual reality) can be utilized. Like other aspects of the Generation IV plant, the HSIs and underlying processing will have to be easily maintained, modifiable, and upgradeable to facilitate introduction of further technological advancements.

Intelligent agents will provide significant support for on-line monitoring, fault detection, situation assessment, diagnosis, and response planning through the use of advanced sensing and computational technology. Detailed, timely, and accurate measurements of overall plant and individual component performance can improve safety and economics by allowing operations and maintenance to be fact based and by reducing the margins needed. Advanced simulators will be capable of taking existing plant conditions and predicting plant behavior faster than in real time. This capability will enable operators to test the response of the plant to alternative actions in order to make better-informed decisions. Further, this will make it possible for the knowledge and experience accumulated from across the industry and throughout a plant's life to be built into systems to support real time design, operations, maintenance, and decommissioning decisions.

HSIs and supporting systems for testing and maintenance should seek to minimize

- maintenance activities (just-in-time maintenance),
- time to maintain,
- impact of production,
- impact on risk, and
- exposure.

Effective testing and maintenance are major drivers for the safety, reliability, and economics of nuclear power. The application of technology to maintenance decision making, planning, and execution has a great potential impact. Some candidate approaches are (1) condition-monitoring sensor technology and software systems that can provide the information needed to make reliability and risk-based decisions for plant maintenance; (2) on-line monitoring and assessment using advanced instrumentation and computational technology; and (3) virtual reality and simulation for maintenance planning. Real-time risk models will be improved and will allow operations and maintenance personnel to optimize surveillance testing and maintenance to ensure risk due to off-normal alignments is minimized.

The following design concepts should enable HSIs to support situation assessment, rapid detection of degraded conditions, response planning, and response implementation.

- Development of methods/tools for information requirements analysis to support supervisory roles and to serve as a basis for developing information systems
- Near-term improvements to HSI resources for alarm processing, information display, soft controls, and computerized procedures (some research is already ongoing)
- Long-term development of highly integrated and intelligent HSIs that combine alarms, information, soft controls to support high-level supervisory role of future “operations” personnel
- Representation systems to support detection of degraded conditions and unplanned/unexpected failures that are based on analysis and human intelligence and experience
- Advanced maintenance interface that uses condition monitoring and equipment databases, to support determination of just-in-time maintenance
- Development of tools for enhanced visualization of status conditions of multiple modules, overseeing multiple simultaneous activities (e.g., use of “data mining” tools in real-time to support the analysis of plant performance data and documentation and the use of predictor displays and fast-time simulation)
- Development of human-computer interaction methods that minimize interface management and navigation workload
- Identification of requirements and applications of portable HSI technology to bring HSIs to where they are needed for monitoring and control may be employed in the future (research consideration should be given to cross-platform compatibility)

Research consideration should be given to portability and transportability and cross-platform capability of human-system interface devices.

3.5.3.3 Knowledge Engineering and Computer-Supported Cooperative Work

It is envisioned that the Generation IV plant will be paperless and that all plant documentation and performance data will be stored in electronic form. Integration and intelligent use of this information will be a significant research topic. Key elements of this research include

- knowledge engineering (knowledge capture and application),
- paperless plant knowledge base (shared and accessible to all functional organizations), and
- computer support for teamwork.

Knowledge engineering involves techniques for identifying and documenting the knowledge of subject matter experts. When this knowledge is coupled with simulation and analysis tools, a powerful knowledge base is created upon which to improve operations and maintenance performance. This information can be applied to the development of more intelligent interfaces in the near term (such as intelligent alarm processing and analysis) to intelligent agent design in the long term. Efficient methods to obtain and store such knowledge in integrated databases are needed.

In addition to improving the technical basis for HSI design, the knowledge base can serve as the platform upon which to coordinate the activities of plant personnel—both locally and remotely. Coordination has been a significant problem in the current fleet of plants, for example, accident precursor events can be caused by unique plant conditions which have resulted from the combined effects of different work groups executing work activities.

In a Generation IV application, the use of computer-supported cooperative work (CSCW) will help minimize these problems. CSCW refers to (1) the use of advanced information systems to supply knowledge within the organization that is needed by different groups to perform work in the most efficient, safe manner, and (2) the use of technology to support crew communication and coordination for advanced reactors. Research is needed to provide tools for real-time use of the plant knowledge base and for CSCW applications.

The elements of this research include the following:

- Determining the means by which knowledge and information can be generated and distributed among work groups
- Determining the means by which work can be conducted and coordinated within a plant complex (i.e., involving multiple plant modules)
- Identifying the principles for use of computer-support tools to enable broad group communication and coordination

3.5.3.4 Research Infrastructure for Human-System Interactions

Limitations exist in the research and development infrastructure that supports the advancement of the research issues discussed previously. The single biggest need is for a research simulation facility. The main simulation facilities available in the United States are the current training simulators. However, these simulators are not available and not suitable for research. The demands on simulation facilities are extreme. Most operate on a 24-hour schedule, providing little available time for research. Further, a large number of plants are expected to significantly upgrade their I&C systems over the next 20 years. Thus, the simulators will be under increased pressure for modification based on plant changes and additional crew training for new control rooms.

Even if training simulators were available, performing research on existing training simulators for Generation IV development would be quite difficult. They are not designed to be flexible,

especially in the area of HSI. Making modification to test novel HSI concepts and fundamentally changing the level of intelligence of the HSIs would be quite difficult.

Ideally, a national research facility should be established. The facility should be coupled with other I&C facility needs discussed in this document. Such an integrated facility will enable the development of integrated human-I&C research. The facility would also provide a platform for proof-of-concept testing and evaluation of all of the research elements previously discussed.

The facility should be developed for and dedicated to research which establishes a set of requirements quite different from training simulators (e.g., the need for flexible modification and data collection are quite different for a research simulator).

3.5.4 Recommendations

Visions for human involvement in Generation IV plant operations have to be identified and analyzed as a technological part of the system in support of overall Generation IV design goals. These visions become design drivers for the development of overall I&C and automation. In addition to the Generation IV vision, an evolutionary migration strategy to achieving the vision should be established to provide proof-of-concepts and to develop public support. An example of such an evolutionary approach is provided in Table 3.5.1.

The development of improved operations and advanced control rooms is important to enhancing public confidence in Generation IV plant designs. For example, demonstrating that the Generation IV plant is operated from a well-designed, state-of-the-art control room will increase public confidence that the plant can be safely operated.

Table 3.5.1. Example of evolutionary development of Generation IV human-system interaction elements

Topic	2002 Generation III plants	2010 Generation III+ plants	2020 Generation IV plants	2040 Generation X plants
Concept of operations	On-site, multi-person crew for one reactor	On-site, multi-person crew for multiple reactors	Decentralized functional groups	Fully-remote operations
Advanced HSIs	Computer-based displays and controls	Intelligent displays and controls	Fully-integrated and intelligent HSIs	Portable HSIs
CSCW	Mainly paper-based procedures and records	Paperless procedures and maintenance	Fully integrated databases and analysis tools	Paperless knowledge bases
R&D infrastructure	Training and vendor engineering simulations	National simulation facility	Multiple simulation facilities for Gen. IV reactor types	Integrated and distributed facilities worldwide

3.6 REGULATORY FRAMEWORK

3.6.1 Session Participants and Goals

3.6.1.1 Participants

Steven Arndt, Nuclear Regulatory Commission
Matt Chiramel, Nuclear Regulatory Commission
Doug Chapin, MPR Associates
Larry Conway, Westinghouse
Arndt Lindner, IST GmbH
Jerry Mauck, Consultant
Ray Torok, Electric Power Research Institute
Robert Uhrig, University of Tennessee, Knoxville
Jim White, Oak Ridge National Laboratory

3.6.1.2 Goals

This session addressed the regulatory infrastructure that will be needed to support the introduction of advanced instrumentation and control systems into the next generation of reactors built and operated in the United States. The goal of the session was to identify what issues and research will be needed to develop a sufficient technical basis to prime the regulators and the industry stakeholders to agree on an acceptable regulatory framework for these new systems and methods.

3.6.2 Overview of the State of the Regulatory Framework

3.6.2.1 Background

Over the past decade, obsolescence of many of the analog I&C system components and equipment and advances in technology have led to an increasing use of digital I&C systems in U.S. nuclear power plants. Newer reactor designs developed and field tested in the 1980s and 1990s, such as the Advanced Boiling Water Reactor (ABWR) and Framatome's N4 Pressurized Water Reactor (PWR) made significant use of digital I&C systems. These systems provide many benefits in operational performance and safety to the nuclear industry. However, the introduction of digital technology into nuclear power plants also presents challenges from a regulatory perspective. These challenges include keeping up with the rapid technology changes, understanding requirements for significantly more complex system analysis and the system's failure modes, and coming to grips with different operational issues.

In recognition of these issues, the NRC updated Chapter 7, "Instrumentation and Control, of NUREG-0800," *Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plant* (SRP) as Revision 4 in 1997. The SRP provides guidance to the staff on how to perform safety reviews of applications to construct and operate nuclear facilities. It establishes criteria and guidelines for both operating plants (modifications) and proposed (advanced) reactor designs. The staff then uses these criteria in evaluating whether an applicant/licensee of a nuclear power plant meets the NRC's regulations. The guidance in Chapter 7 is currently used for the review of both advanced reactors and plant-specific digital retrofits of current-generation plants; however, it was not written with the newer, next-generation reactor designs in mind.

The new generation of advance reactor concepts, both for HTGRs and ALWRs, will be the first opportunity for vendors in the United States to build new reactor control rooms. The advances used in the development of many of the current generation of operating reactors in other parts of the world will be used in the design and construction of new plants. In addition, the desire for

much smaller staff size for the control room will push power plant designs toward more automation (similar to the changes in the fossil-fired power plants). The use of multiple modular plants may also require more complex control of both the primary I&C systems and of all of the support systems, including the switchyard. Additionally, a more risk-informed regulatory framework could potentially be used in the licensing of these advanced plants.

3.6.2.2 Overview of Technical Topics

The NRC Research Plan for Digital Instrumentation and Control (SECY-01-155) outlines current and future research in several areas of emerging I&C technology and applications that will be used in the HTGRs and ALWRs. Research will include smart transmitters, wireless communications, advanced predictive maintenance, on-line monitoring methods, and enhanced cyber security issues. This research will support the development of review guidance for the NRC Office of Nuclear Reactor Regulation (NRR) and will address these new and improved technologies and will apply to both current reactors retrofits and advanced reactors.

The national and international research community has been involved with research and development of advanced control and monitoring systems for nuclear power plants for many years. The international community, particularly Europe, Japan, and Korea, have developed integrated advanced control rooms and have performed more research in the areas of automation of plant operations and advanced plant monitoring and diagnosis than has been done in the United States. Therefore, significant opportunities exist for international cooperation in this area. General Atomics is studying detailed control systems design using plant simulators to help optimize control system designs. PBMR Corporation is also looking into advanced control systems. These research and development efforts are being performed by both the vendors and joint teams that include other research organizations such as universities and U.S. national laboratories, including Oak Ridge National Laboratory (ORNL) and Idaho National Engineering and Environmental Laboratory (INEEL). I&C design is one of the major areas of research outlined in DOE's long-term nuclear technology research and development plan. Several of the research topics proposed in this plan are of particular interest to HTGRs, such as robust communications and wireless sensors, smart instrumentation, and condition monitoring. Also of interest is research into distributed computing, condition monitoring, advanced control algorithms, and on-line monitoring. As part of the implementation of this long-term research plan, DOE has developed six Nuclear Energy Research Initiative programs in this area. These include research in the areas of automatic generation of control architectures, self diagnostic monitoring systems, smart sensors, and advanced instrumentation to support HTGRs.

The advanced reactor plants will be designed for autonomous operation using a minimum of supervision by plant operators for long periods of time. This may include automated startups, shutdowns, and changes of operating modes. Using fewer staff will require that both normal operations and off-normal operations and recovery be more highly automated. To make modular reactor concepts effective, the plant must work like a single, larger plant. This will require a level of automation and coordination that is heretofore unheard of in the nuclear power industry. The current regulatory structure was not developed with this kind of operating profile in mind. The regulatory structure will need to be reviewed and current regulatory guidance expanded or enhanced to facilitate better understanding of how plant control and safety systems will be designed to cope with partial failures of interconnected systems, particularly at the switchyard and the control room.

Because of the longer fuel cycles and much longer time between maintenance outages, the plants may use more extensive on-line monitoring, diagnostics, and predictive maintenance. Instrumentation will be needed to support this increased automated surveillance. How these

systems will integrate into the regulatory structure will need to be reviewed. Because some of the systems in this new generation of ALWRs and HTGRs will be operating in new temperature ranges, it is expected that several new kinds of sensors will be developed. The limitations of these new sensors will need to be investigated. A new generation of temperature, pressure, flow, and neutron detectors may require changes in the methods for performing design and safety calculations (drift, calibration, response time, etc). Current regulatory guidance and tools will need to be reviewed and enhanced to support the review of these systems.

The application of highly automated control rooms in other industries has used modern control theory controllers to increase plant availability and decreased the operators' workload. These new HTGRs are likely to use some of these advanced modern control methods. These could include simple feed forward controllers, nonlinear controllers, neural-fuzzy controllers, or even more exotic methods. How these control algorithms will affect the operational modes of the plants need to be investigated. Additionally, review guidance and tools need to be developed to analyze these methods.

To adequately understand the more complicated digital I&C systems within a risk-informed licensing framework, additional risk modeling is needed. This capability will also be needed to support operator-control interface research. Because of the lack of adequate models and data to support risk analysis, the uncertainties in this area are relatively high and can only be reduced by significant new research in this area.

3.6.3 Issues and Needs for the Regulatory Framework

The working group experts reviewed the current state of both technology and the regulatory infrastructure. Based on these discussions, the consensus was that the current regulatory structure can support moving forward into the higher levels of capability and complexity made possible through the use of new I&C systems—systems that will be needed for Generation IV reactors. However, several regulatory infrastructure areas need to be improved to support advanced I&C and human factors elements for advance reactor systems.

3.6.3.1 Improving Regulatory Effectiveness

Providing a more effective, efficient, and cost effective regulatory framework and maintaining regulatory knowledge infrastructure requires focusing on the most risk-important issues and using tools and models to improve regulatory timeliness.

Risk-informed regulatory processes are needed for IC&HMI, including a process for integration and interfaces with plant PRA and a process for a risk-based graded approach for IC&HMI regulation. This risk-informed regulatory process should include development of better

- risk models for digital systems, specifically software;
- data to support PRA modeling of digital systems, specifically software; and
- screening criteria for including I&C systems in PRAs.

Knowledge is needed to support revision of the NRC SRP and to support other software development models (e.g., nonwaterfall). Investigation of alternate software development models is needed, and benchmarking of alternate methods to support regulatory submittals of nonwaterfall methods needs to be done. The timeliness of regulatory guidance updates (“living guidance”) also needs to be improved. Other needs include (1) investigating alternative to consensus standards endorsement process, including nuclear industry specific guidelines, (2) benchmarking other regulatory agency I&C methods, and (3) developing new pilot processes, using an ITAAC as an example.

New methods are needed to address updating of equipment (and software) by vendors and licensees to account for obsolescence, on a time scale appropriate to I&C product updates. These methods should consider the appropriate time scale for nuclear I&C products and ways to deal with planned outage schedules.

New “standard” review technique are needed to avoid repetitive custom reviews of I&C systems (i.e., more efficient reviews). This development of a new standard should include the review of existing requirements to extract more precise requirements (reduce complexity), more quantitative requirements, a “sample” SER for advanced I&C systems, and better assessment and testing tools.

3.6.3.2 Regulatory Assessment of I&C systems

To effectively implement regulatory improvement, new methods, techniques and tools to assess I&C systems and their characteristics will need to be developed.

Improved methods are needed for assessing development and testing tools used by the vendors of new I&C systems. The regulators will need to develop improved assessment methods applicable to test and development tools (analogous to those for compilers) and define the applicability of assessment tool to risk appropriate levels.

Better failure data and reporting methods are needed to support operating failure information, best practices, and reliability data. Research should be started to develop standards for collecting and reporting failure data for digital systems and for developing tools to analyze digital systems failure data and define/promulgate best practices.

Most importantly, an improved reliability assessment method is needed that includes testing for high reliability systems (graded approach). The research ongoing at the University of Virginia and in other research programs needs to be continued and expanded. This and other work should be reviewed to determine its adequacy for use in the regulatory process. This work can best be done in collaboration among DOE, NRC, and the vendors.

This work should also include the development of assessment methods for nondeterministic systems, including intelligent agents, adaptive systems, and neural networks. The research should include development of methods for determining failure modes and unanticipated and undesired behavior and development of acceptance criteria.

3.6.3.3 New Plant I&C Issues

As new plant designs are completed, the need to ensure regulatory framework and infrastructure to support new plant issues (i.e. multiplant designs, higher temperatures, new failure modes) is apparent. An ongoing research effort is needed to define and develop the additional regulatory information necessary to support different plant behavior, operating modes, hazards, and mitigation features (Chapter 15 events and accidents).

Based on review of new plant designs and PRAs, research should start by defining R&D issues for I&C, such as, qualification issues, design-basis accident criteria for I&C system, and I&C requirements for demonstration plant (license by test) applications.

The research should focus on providing information needed to support the development of acceptance criteria. This will include research into both new plant design traits and the uses of I&C to accomplish improvements in plant operations and economic viability.

The current regulatory structure does not address nontraditional plant design features that may be important to safety in Generation IV reactor designs, such as fuel QA in HTGR. Based on review of new plant designs and PRAs, R&D issues for I&C associated with nontraditional plant features, such as the need to have safety instrumentation as part of fuel manufacturing, will need to be studied. Development information to support regulatory analysis and setting of acceptance criteria is also needed.

In addition regulatory information is needed to support review of multi-modular plants, including shared systems (e.g., safety, control and/or information systems), operator interfaces in multi-modular control rooms, IE power supplies, etc. Based on review of design, research should include an evaluation of potential regulatory issues associated with multi-modular plants and the development of regulatory guidance to review risk important multi-modular I&C issues

Trial evaluation of one or more reactor systems to determine what impact inherent safety features will have on I&C requirements should be carried out. In this way, additional regulatory requirements or regulatory relief will be identified. New methods for assessing instrumentation system performance in new plant environments (such as, high temperatures, different EMI issues for wireless) will also need to be developed. These assessment methods will include defining research and development needs such as confirmatory testing requirements and should be done in concert with DOE, industry, NRC, and others in the nuclear power plant industrial sector. The development of new assessment methodology will also be needed for

- determination of adequacy of instruments for long-term operation (long cycles);
- use of the plant over extended time periods (aging);
- confirmatory testing requirements and information gathering; and
- supporting first-of-a-kind and demonstration plants.

3.6.3.4 Emerging Technologies

As new digital technology is now replacing old analog systems in current generation nuclear power plants, emerging technology will replace the systems being proposed for implementation in the next generation of plants, in some cases, before the plants are even built (e.g., AP600). A forward-looking research program to ensure regulatory readiness for implementation of emerging technologies is needed.

Review guidance is needed for advanced surveillance methods (self test, on-line calibrations, early fault detection, adaptive systems, etc.) as well as for issues that could cause vulnerability to cyber attack. Regulatory requirements and assessment methods for cyber security issues need to be improved and should include

- identification of safety-significant cyber security threats,
- development of acceptance criteria for safety-significant cyber applications, and
- development of assessment methods for cyber security.

New methods and information to support licensing of robotics for maintenance, inspection, fuel handling, etc., need to be developed. Methods are also needed for determining failure modes and unanticipated or undesired behaviors and methods for developing acceptance criteria.

Regulatory guidance must be created in the area of use of digital media for documentation and data storage, configuration control, and storage of control algorithms in computer chip. Other issues to be dealt with include aging and degradation, evaluation of degradation of digital storage media, and determination of the effects of degradation on safety-significance. Regulatory guidance and information also needs to be developed to support wireless technology and distributed control and information system (e.g., information flow, information sharing). This

guidance information would include a (1) a better understanding of operational limitation of the technology, (2) knowledge about the safety impact of use of systems in new reactors, and (3) an understanding of regulatory acceptance criteria and assessment methods. Regulatory information concerning the use of new technologies to support configuration control, maintenance, security, etc. (e.g., video, biometric) is also needed.

3.6.3.5 Human System Interfaces and Other Operational Issues

As the type, style, and operation of HSI and the roles of the operator change so too does the regulatory structure needed to support their design and implementation. Research to support possible revisions of the regulatory structure should be carried out.

Developing improved methods will be needed to assess hybrid control rooms (including the definition of requirements for safe operation). Hybrid control room research is on-going for current plant upgrades. Assessment of applicability to new reactors such as multi-modular plants to the current regulation will be the first step. A better understanding is needed of new features, new behaviors, and new failure modes (and unanticipated and undesired behaviors) associated with advanced control rooms using advanced HSIs. Based on research in this area, new regulatory guidance for advanced HSIs and an assessment methods to ensure appropriate application of advanced HSIs are needed.

Regulatory guidance will be needed to help establish the allocation of functions between the operator and the advanced control systems and to further the development of improved cognitive operator models that can be used in the assessment of advanced designs. Also needed is support of human reliability assessment models for advanced reactor designs and support for new requirements and regulatory guidance for review of operator and advance control systems, relating to functional allocation.

A definition of requirements and regulatory guidance should be developed for different operational allocation of duties during off-normal conditions in new plant designs, including off-site experts, interactions with corporate offices, or support from other module staff (operator licensing), as well as guidance to support review of possible new distribution of functions.

3.6.4 Recommendations

The research described in previously in this section can serve as the basis for numerous projects directed toward the stated goal of providing a technical basis for regulatory acceptance of the application of these new technologies. DOE should, in cooperation with the NRC, provide research to support risk-informed regulatory processes for IC&HMI; and integration and interfaces with plant PRA and risk-based graded approaches for IC&HMI regulation should be its highest priority. DOE and NRC should coordinate activities to develop information and tools needed to update the regulatory framework, develop new techniques and tools to assess I&C systems and their characteristics and demonstrate their capability, and proactively work to ensure that information is available to support the regulatory framework and the infrastructure updates for new plant issues and emerging technology.

4.0 MEETING RESEARCH NEEDS—A PROPOSED PATH FORWARD

4.1 HIGH PRIORITY PROJECTS, FACILITIES, AND TEST BEDS

4.1.1 Goal

The overall research objectives developed by each of the working groups can be best realized by providing facilities for demonstration of key enabling technologies for the application of advanced instrumentation and controls, human-machine interface systems, and other interface systems to support selected NP2010 designs (e.g., one water and one gas-cooled design) and by providing the foundation for Generation IV applications through targeted, high-priority research projects. It is clear that development of comprehensive research facilities and test beds cannot be the primary focus of an IC&HMI research effort because that might detract from the many benefits to be gained from immediate application of advanced technology and methods via modest projects. Nevertheless, a “virtual” research complex can be assembled from existing distributed research resources and facilities that can provide integrated access for coordinated research activities. The capabilities of this virtual test bed can then be expanded through addition of new resources as part of individual research application projects under NERI, INERI, NP2010, international near-term deployment, or Gen IV projects. It is the recommendation of the IC&HMI Workshop participants that existing research capabilities be surveyed, an advisory committee to coordinate interaction and access be established, and research projects, based on the described research needs, be funded to contribute any missing elements of the overall test bed capability.

4.1.2 Demonstration Program for NP 2010

The workshop participants suggest that DOE-NE solicit proposals for a “Program for Research and Demonstration of Advanced Instrumentation, Controls and Human Machine Interfaces for Next Generation Nuclear Power.” This would address needs of both gas-cooled and advanced water reactor systems and would be a step towards demonstrating technologies needed for international near-term deployment and Generation IV power plants. The following recommended demonstration activities address enabling I&C technologies that will be needed to facilitate the design, construction, and operation of new reactors.

- Testing and qualification within the selected environment of advanced sensors for critical measured variables important to the safe and reliable operation of the respective selected design
- Demonstration of integration of multiple field bus elements with control and display features
- Development of testing protocols for quantification of uncertainty in diagnostic and prognostic modules applied to the selected test bed sensors and control system
- Development and demonstration of a hybrid diagnostician for forward and backward propagation with prognostic correlation of selected faults associated with the selected control system
- Demonstration of intelligent hierarchical control that integrates diagnostic information with control decisions for the selected control system
- Demonstration of varying levels of autonomy of the overall plant control system
- Demonstration of the generation of software specification from system requirements using the sequence-based specification technique
- Application of the model-based statistical testing for the quality certification of the selected software

- Development of in-parallel regulatory review and acceptance guidelines for the selected system diagnostics, etc., including integration with risk-informed, performance-based regulatory initiatives
- Development of improvements to the regulatory structure accounting for new operational modes of the plant
- Development and investigation of strategies for functional allocation in highly autonomous, adaptive control systems
- Development and evaluation of intelligent HMI technology to support event detection and situation assessment for operational and maintenance applications

A coordinated demonstration program will advance the state-of-the-technology while contributing to the establishment of a test bed capability. The resources developed through this program would be linked to hardware that is based on selected NP 2010 Initiative designs. Together, the hardware and I&C elements will provide the basis for more general-purpose test bed platforms that can be utilized for complex, innovative research and development.

4.1.3 Longer-Term Research Areas Supporting Generation IV

In addition to research to support the NP 2010 Initiative, additional high-priority goals for supporting the development of Generation IV nuclear power reactors are summarized as follows:

- Evaluate sensor communication pathways and material challenges related to radiation-hardened electronics
- Assess various signal processing methodologies
- Develop guidance for autonomous system network design, management and control
- Identify necessary characteristics and investigate means for accomplishing interoperability of computing and communication architectures over the design lifetime to minimize impact of digital system obsolescence
- Develop and validate degradation models for selected materials and system elements
- Determine capabilities and limitations for the use of advanced inverse algorithms for parameter determination in diagnostic schemes
- Investigate unique control characteristics of multimodular plant implementation
- Demonstrate self maintenance for an advanced control system
- Develop and demonstrate comprehensive systematic methods for quality determination (attributes and measurement) of software-based systems
- Develop and demonstrate integration of digital system reliability modeling and PRA models
- Develop and demonstrate systematic methods for evolving advanced concepts for operations and staffing that reduce cost and maximize safety and productivity
- Develop and demonstrate advanced HMI concepts to intelligent support for enhanced monitoring, situation assessment, response planning, implementation, and coordination/communication of human and intelligent agents in highly automated, multimodular designs.
- Develop and demonstrate risk-important design methods for IC&HMI systems in modular and shared systems concurrently with the development of risk-informed regulatory guidance for their review.

The IC&HMI Workshop participants recommend the above research activities as high priority project ideas that will promote the realization of advanced designs for both international near-term deployment and Generation IV reactors.